Department of Defense
Defense Information Systems Agency
Wireless Security Support Program

Wireless LAN Security Framework

January 2004

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

As wireless technologies and devices proliferate, they can pose significant risks to national security and to the non-wireless networking infrastructures if not properly implemented and secured. Experience has shown that as new technologies are developed, they become a major source of new vulnerabilities for which security solutions must be developed. Wireless local area networking (WLAN or "WiFi") is one of the wireless technologies that present great opportunities as well as security concerns. To assist in the secure deployment and operations of 802.11 WLAN technologies, the Defense Information Systems Agency (DISA) has created a Wireless LAN Security Framework. This guidance provides a common conceptual framework to assist the Department of Defense (DoD) in coordinating acquisition, development, architecture design, and implementation of 802.11 wireless infrastructures connected to the Non-Classified Internet Protocol Router Network (NIPRNet).

The framework discussed in this document is geared to developers, system architects, system administrators, and system users. The framework is intended to guide the secure design, development, and implementation of WLAN security technologies that comply with relevant DoD policy. This document defines WLAN components for a secure WLAN solution and discusses proper implementation.

1.1 SCOPE

The framework presented in this document can be applied to all DoD WLANs in unclassified environments (e.g. NIPRNet). It is intended that this WLAN framework will result in common architectures and security solutions that will be secure, flexible, and interoperable as future standards and technologies evolve.

1.2 AUDIENCE

This document provides a conceptual framework for implementing WLANs securely. In doing so, this document covers details specific to WLAN technologies and solutions for a secure connection to the NIPRNet. The content is technical; however, this document provides the necessary background information to aid readers in understanding the topics discussed. The following list highlights how people with different backgrounds and roles might apply the guidance in this document. The intended audience is varied and includes the following:

- Government managers who are planning to employ a WLAN in their agency (such as chief information officers or senior managers)
- Systems engineers and architects who are designing and implementing a WLAN for an unclassified environments

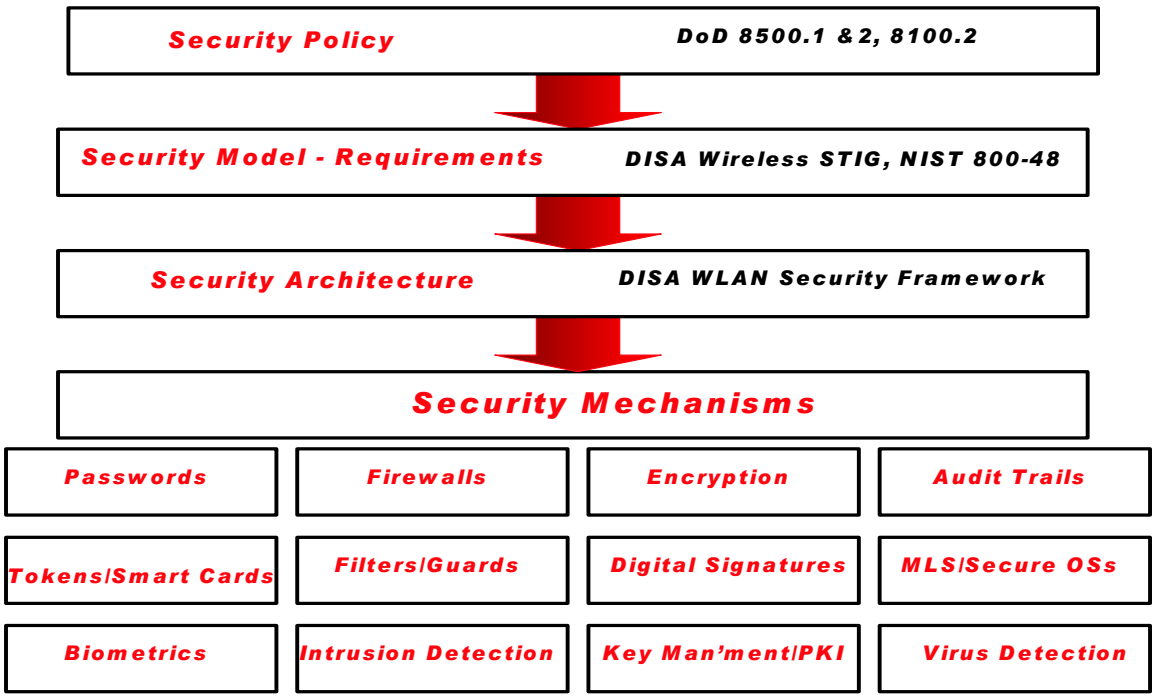
- System administrators who are administering, securing, or upgrading the WLAN connected to the NIPRNet
- Security consultants who are performing assessments to determine security postures of unclassified wireless environments.
- Wireless users who are interested in understanding the security issues surrounding WLANs and the mechanisms used to mitigate that risk.

This document assumes that the readers have minimal operating system, networking, and security expertise. Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to these technologies, readers are strongly encouraged to take advantage of other resources for more current and detailed information.

1.3 APPROACH

This document follows a standard security engineering approach where high-level requirements are dictated by security policy. These requirements are then translated into a conceptual architecture. Once the architecture is defined, specific security mechanisms can be selected. Figure 1-1 depicts this approach and the specific application to the WLAN Security Framework.

Figure 1-1. Security Engineering Approach to WLAN Security Framework



The policies on which this framework is based include the DoDD 8500.1, DoDI 8500.2, and DoD Wireless Security Policy 8100.2 (Draft). The DISA *Wireless Security Technical Implementation Guide (STIG)* and National Institute of Standards and Technology (NIST) Special Publication 800-48 on *Wireless Security of 802.11, Bluetooth, and Handheld Devices* are used as references, which provide specific requirements used to define secure WLAN architecture. This architecture makes up the WLAN Security Framework.

The WLAN framework also discusses functionality of the security components. DoD entities using this framework should be able to select the solution that best fits the requirements of their environment and successfully implement a secure network.

It is expected that in future STIGs and guidance documentation, DISA and the DoD will provide detailed guidance for the configuration of the specific WLAN security products.

1.4 DOCUMENT STRUCTURE AND USE

This document is divided into 12 sections. After the introduction and background, this document continues with a presentation of the WLAN security framework, then discusses implementation considerations and some of the framework's critical mechanisms in following sections, and then concludes with checklists that are intended to serve as functional tools to assist agencies when implementing applicable solutions.

The following tables provide an overview of the document and assist in its use. Table 1-1 maps each section of the document to a general synopsis of its content.

Table 1-1. Document Roadmap

Section	Title	Description
Section 1	Introduction	This section includes the purpose and scope of the Wireless LAN Security Framework.
Section 2	Background	This section provides additional background information and a short discussion of threats and vulnerabilities.
Section 3	Policy and Guidance	This section highlights the relevant policies and guidance available for reference when implementing a wireless infrastructure.
Section 4	WLAN Framework	This section discusses the WLAN framework and four ways this framework can be implemented.
Section 5	Implementation Considerations	This section discusses items that must be considered prior to design and implementation. Some of the items that must be considered include Certification and Accreditation, Common Criteria, scalability and interoperability, proprietary vs. standards-based solutions, and future considerations.
Section 6	Administrative Controls	This section focuses on some of the key administrative controls that must be implemented to adequately secure WLANs.
Section 7	Technical Mechanisms	This section discusses some of the key technical mechanisms that are included in the reference model and must be considered during design, testing, and implementation of a WLAN.

Section	Title	Description
Section 8	Mobile Device Security	This section discusses the security that is critical to the secure use of mobile devices.
Section 9	Future Considerations (802.11i)	This section discusses that 802.11i access solutions are expected to be the solution of the future.
Section 10	Case Studies	This section includes case studies that describe how wireless LANs are currently being securely deployed in the DoD. These case studies relate to one of the four ways that the WLAN framework can be implemented
Section 11	Checklists	This section provides checklists that are intended to provide guidance when procuring and implementing WLANs.
Section 12	Acronyms	This section provides a list of the acronyms used in the document.

Table 1-2 discusses the intended purpose for the various sections of this document.

Table 1-2. Document Use

Section	Use	Focus
Section 1 & 2 (Introduction and Background)	Read these sections to understand the scope and purposes of the document and to learn about some of the threats and vulnerabilities addressed by this document.	Overview and Background Information
Section 3 (Policy and Guidance)	Read this section to gain an overview of the policies used in development of the framework.	Policy
Section 4 (WLAN Security Framework)	Read this section to understand the general architecture and components used in the WLAN Security Framework.	Conceptual Architecture
Sections 5 through 9	Read these sections to gain an understanding of some key implementation considerations, key technical mechanisms, key administrative controls, mobile device security, and future considerations.	Security Mechanisms
Section 10 (Case Studies)	Read this section to gain an overview of some existing WLAN implementations in the DoD.	Existing WLAN Implementation
Section 11 (Checklists)	Use the checklists in this section as tools during the design and engineering of a WLAN. A C&A checklist is provided which presents the steps that must be taken as a part of the design and implementation of a WLAN to provide a secure system that is approved for use. A product selection checklist is provided that includes key components that each of the security products used in a WLAN must support. A WLAN Security Checklist from the NIST Special Publication 800-48 is included. This checklist provides detailed management, technical, and operational recommendations that should be addressed as a part of any WLAN design and implementation.	Checklists to facilitate product selection and implementation
Section 12	Use this section as a reference for acronyms used in this document.	Acronyms

2. BACKGROUND

The NIPRNet was developed to enable existing services and DoD agencies to exchange unclassified information. With the proliferation of WLAN technologies, significant emphasis has been placed on security because of the flawed initial design of the security components of the 802.11 protocol. Even with the concerns about security, the benefits of WLANs have driven the adoption of this technology in commercial and government arenas.

To effectively implement WLANs in the DoD, WLAN architecture must be designed to address related threats and vulnerabilities. As with any wireless communication, an attack based on passive collection and traffic analysis cannot be fully mitigated. This attack, however, will not result in data compromise or provide an attacker access to the network. All attacks that result in a compromise of data or unauthorized access can be mitigated. Table 2-1 lists common WLAN attacks that are considered in the WLAN Security Framework. It is important to note that strong encryption, strong mutual authentication, and other controls that work together to provide layered security are included in this framework. The following table provides only a high-level view of the attacks and mitigations:

Table 2-1. Common Attacks on Wireless Networks

Attacks	Comment
Traffic Analysis	Only wireless client and access control devices addresses (MAC or IP) are visible to an adversary; all other traffic is encrypted.
Passive eavesdropping	Strong encryption will prevent eavesdroppers from being able to collect any usable data.
Partial or known plaintext attack (e.g., Wired Equivalent Protocol [WEP] attack)	This is not a concern because in this framework WEP is not used to provide encryption.
Unauthorized Access	This attack is mitigated by strong authentication and FIPS 140-2 encryption.
Man in the Middle	This is mitigated by mutual authentication and strong encryption. A successful man-in-the-middle attack is defined as the capture of encrypted data and successful decryption of the data.
ARP Attacks	This attack is mitigated through strong mutual authentication and FIPS validated encryption.
Replay Attacks	This is mitigated by strong authentication and encryption. Also, protocols such as IPSec, TKIP and CCMP have a counter for replay protection built into packets.
Session Hijacking	This is mitigated by strong encryption and authentication mechanisms.
Redirection	Any plaintext IP addresses should be non-routable.
Denial of Service	Incidence response is key to minimizing impact.

3. POLICY & GUIDANCE

This section highlights the relevant policies and guidance available for reference when implementing a wireless infrastructure. These policies were considered and incorporated into the WLAN Security Framework.

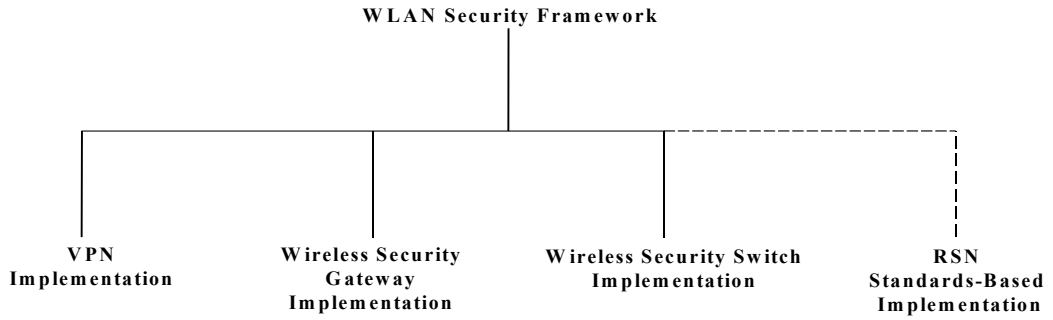
Policy	Description
DISA Wireless STIG	The DISA STIG is published as a tool to assist in the improvement of the security of DoD information systems. The guidance provided in the STIG is authoritative according to DoD Directive 8500.
DoD Directive (DoDD) 8100.2 (Draft)	Describes the appropriate use of use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG)
DoD Directive (DoDD) 8500.1	Prescribes the use of information assurance in a defense-in-depth approach
DoD Instruction (DoDI) 8500.2	Implements policy; assigns responsibilities and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoDD 8500.1.
DoD Instruction (DoDI) 5200.40	DoD Information Technology Security Certification and Accreditation Process (DITSCAP), http://iase.disa.mil/ditscap/ditsdocuments.html, is required for any new IT system. It is used to implement policy, assign responsibilities, and prescribe procedures for Certification and Accreditation (C&A) of information technology (IT), including automated information systems, networks, and sites in DoD. The System Security Authorization Agreement (SSAA) is key to the DITSCAP. The SSAA is used to guide and document the results of the C&A and the implementation of IT security requirements. It resolves several issues including the critical schedule for the C&A, the budget, security requirements, functionality of the system, and performance issues.

4. WLAN SECURITY FRAMEWORK

Effectively securing a WLAN begins with an architecture that incorporates all of the DoD policy-based administrative controls and technical mechanisms discussed in Sections 7 and 8. However, many practical factors such as scalability and cost also need to be considered during the design process.

The WLAN Security Framework provides reference implementations that should be used by network designers to ensure the tenets outlined in Sections 7 and 8 are incorporated in their design. Further, practical considerations of each implementation are discussed to assist in the decision-making process. This section will outline the four reference implementations shown in Figure 4-1.

Figure 4-1. Framework Taxonomy



All of these implementations have a similar component set and architecture. What distinguishes them is the specific component (referred to as the access control device) that provides a number of essential security features to the architecture. As evident in Figure 4-1, the access control devices that will be discussed include a Virtual Private Network (VPN) Device, Wireless Security Gateway, Wireless Security Switch, and Robust Secure Network (RSN) standards-based device.

In the next subsection, the framework architecture will be covered, including the basic network components and their important features and configurations. Subsequent sub-

sections will provide a discussion of each specific implementation, including benefits and limitations of each.

4.1 WLAN SECURITY FRAMEWORK ARCHITECTURE

This section describes the WLAN framework as the basic architecture that can be used as a model for deploying wireless networks in DoD unclassified environments. A number of network components are needed to implement all of the critical mechanisms to secure a wireless network. Figure 4-2 shows the components required to implement the generic architecture. As discussed previously, all components are common to all implementations of the WLAN framework except the access control device.

Figure 4-2. Basic Components

4.1.1 Wireless Client

The wireless client provides the user interface for networked applications (e.g., Web browser, e-mail client) as well as wireless communication capability via a wireless network interface card (NIC).

The wireless NIC installed in the wireless client should be 128-bit Wired Equivalent Protocol (WEP) or WiFi Protected Access (WPA) capable. This will allow encrypted communication between the wireless client and access point using the maximum WEP/WPA key size available. Because neither WEP nor WPA is compliant with Federal Information Processing Standard (FIPS) 140-2 (see Section 7.2), this will not completely satisfy the policy requirement regarding encryption. However, this encrypted communication between the client and the access point will add a layer of security to the network. If available, an additional desired feature of the wireless NIC would be IEEE 802.1x and/or IEEE 802.11i capability. See section 4.5 for the reference implementation using IEEE 802.11i RSN-based devices.

The wireless client must be Common Criteria certified against any existing Protection Profiles (see Section 5.1). The wireless client will also need to be configured in compliance with all applicable STIGs. STIGs are available for a number of common operating systems and applications. Since wireless clients are available on different types of devices (e.g. notebook computer, PDA), a determination would need to be made as to which STIGs apply to each type of client. In all cases, software installed on wireless clients should be routinely inventoried and assessed for STIG compliance.

The primary encryption mechanism on the wireless client will be software and/or hardware that provide file system and tunneling encryption capabilities. File system encryption will provide storage security while the tunneling encryption will secure the communication between the client and the network.

The wireless client must be configured with host-based countermeasures such as a personal firewall, intrusion detection system, and virus protection software. These countermeasures will allow the device and the user to determine imminent or active attacks against the wireless client.

For further protection, file- and printer-sharing functionality must be disabled. There are numerous known attacks for these features that are further susceptible to wireless devices.

Table 4-1 is a summary of the features/configurations for the wireless client.

Table 4-1. Wireless Client Features/Configuration

Wireless Client Features/Configuration	Required	Recommended
Common Criteria certified against any existing Protection Profiles	✓	
Applicable STIG compliance (e.g., operating system, applications)	✓	
Wireless NIC is 128-bit WEP/WPA capable.		✓
Wireless NIC is IEEE 802.1x and/or 802.11i capable (if available).		✓
Encryption client software (FIPS-140-2 certified) for storage and communication security.	✓	
Personal firewall	✓	
Intrusion Detection System (IDS)	✓	
Virus protection	✓	
File/printer sharing disabled.	✓	

4.1.2 Access Point

The access point provides the wireless client with access to the wired network. It consists of a radio interface (to communicate with wireless devices), a wired network

interface (to communicate with wired devices), and bridging software to pass information between the two interfaces.

Most commercially available access points include a number of features that need to be securely configured. Normally, these features are administrated via a Hyper Text Transfer Protocol (HTTP) or Simple Network Management Protocol (SNMP) interface that is password protected. This is convenient during initial setup, but those interfaces should be considered a security risk after that. Therefore, it is a recommended practice to disable all non-cryptographically protected management interfaces (e.g. HTTP) once the access point is configured. If management access is required or desired on a regular basis, a secure cryptographically protected interface should be used (e.g. SSH, HTTPS).

The wireless access point must be Common Criteria certified against any existing Protection Profiles (see Section 5.1).

The access point should be 128-bit WEP or WPA capable for encrypted communication with the wireless clients. As discussed with the wireless client, this encryption will not satisfy policy requirements but will add a layer of security.

A Service Set Identifier (SSID) is a configurable name associated with an access point to identify the wireless network it supports. The SSID is broadcast in plaintext during beaconing and probing—both activities advertise the access point's presence to potential clients—as well as during communication with authorized devices. Hence, it is a trivial exercise for unauthorized users within communication range of the access point to capture the SSID.

Therefore, the SSID should not be set to a name that provides information about the network the access point services (e.g., Company "A" Wireless Network). This information may provide an adversary with information that would facilitate an attack. The SSID should be a random string of characters, preferably compliant with DoD network password rules. As an additional measure, the SSID broadcast feature must be disabled.

To perform any attack on a wireless network, an adversary first needs to be within reception range of a wireless device. To minimize the range of the access point, it is essential that the transmission power be set to the lowest possible setting. Signal testing will be required to ensure that authorized users/devices can still communicate with the access point at a lower setting. The idea is to minimize the signal power as much as possible to prevent unauthorized access.

In the 2004–2005 time frame, the 802.11i standard should be finalized and implemented in commercial products. 802.11i will be a major improvement to wireless security in terms of encryption and authentication mechanisms. Therefore, it is recommended that 802.11i-enabled access points (when available) be used in any implementation.

Table 4-2 is a summary of the features/configuration for the access point.

Table 4-2. Access Point Features/Configuration

Access Point Features/Configuration	Required	Recommended
Common Criteria certified against any existing Protection Profiles	✓	
128-bit WEP/WPA capability		✓
SSID beacon mode disabled		✓
Pseudo-random SSID, preferably compliant with DoD network password rules		✓
HTTP/SNMP management access disabled; ensure only secure management access is available (e.g., SSH).		✓
Transmission power set to the lowest possible setting that will meet the required signal strength for the service area	✓	
802.11i[1] security capability (when available)		✓

4.1.3 Radio Frequency Monitor

The radio frequency (RF) monitor provides a periodic snapshot of the wireless environment, helps to identify rogue access points, and/or acts as a wireless Intrusion Detection System (IDS) for the WLAN. It monitors the RF space (in this case, the 802.11 frequencies) and analyzes the communication traffic for notable events in real time. RF monitoring must be performed in at least one of two possible manners: periodic or continuous scanning. Continuous scanning is highly recommended for maximum effectiveness.

The RF monitor should be able to recognize known network attacks (e.g., denial of service, port scans, man in the middle) if a device that provides an IDS capability is used. A knowledge base of attack signatures needs to be stored on, or made accessible to, the RF monitor. Because of the dynamic nature of this information, the knowledge base should be capable of being updated in a straightforward manner (e.g., software/data download).

The RF monitor should to be able to detect rogue access points or other unauthorized devices. A straightforward approach would be to verify the media access control (MAC) addresses of all wireless devices against an access control list (ACL). Because MAC address spoofing could circumvent this approach, a more sophisticated mechanism (e.g., certificate-based) may be desired.

Depending on the event detected, a network administrator needs to be notified as quickly as possible. In the case of a network attack or rogue devices, a real-time alert mechanism (e.g., pager) is essential. There is a small window of opportunity after the event is detected to thwart the attack and possibly apprehend the attacker. At a

[1] *Institute of Electrical and Electronics Engineers (IEEE) 802.11i Specification*

minimum, the RF monitor should log all information related to the event (e.g., timestamp, MAC address).

It would be beneficial for the RF monitor to be integrated into an existing, centralized incident response system. It is generally more cost-effective and easier to maintain a centralized system than multiple, independent systems.

The RF monitor must be Common Criteria certified against any existing Protection Profiles (see Section 5.1).

Table 4-3 is a summary of the features and configurations for the RF monitor.

Table 4-3. RF Monitor Features/Configuration

RF Monitor Features/Configuration	Required	Recommended
IEEE 802.11 signal detection	✓	
Continuous scanning capability		✓
Attack signature recognition (updateable)		✓
Rogue access point /client detection		✓
MAC address ACL verification		✓
Audit logging capability		✓
Real-time alert mechanism (e-mail, pager, etc.)		✓
Integration with centralized monitoring and management systems		✓
Network health verification (e.g., interference, slow performance)		✓
Common Criteria certified against any existing Protection Profiles	✓	

4.1.4 Access Control Device

The access control device must be Common Criteria certified against any existing Protection Profiles (see Section 5.1).

The access control device needs to provide network access control. Until a client has been authenticated and authorized, the device should not allow traffic from that client to pass onto the wired LAN (or vice-versa). This functionality may be provided by an integrated network firewall or other network access control mechanism.

The access control device authenticates the wireless client to the network. This process begins by the client passing its credentials to the access control device during the network login phase. Depending on the authentication protocol being used, the device communicates with an authentication server to determine if the client credentials are acceptable and passes the results to the client.

Once authentication is complete, the access control device constructs the encrypted tunnel with the wireless client that the session traffic will pass through. This process sometimes involves encryption algorithm and protocol negotiation.

The device should have a logging capability for documenting events such as client logins/logoffs, failed logins, and unauthenticated/unauthorized traffic.

To prevent session hijacking, the access control device should time-out sessions that are inactive for 15 minutes. Local security policy may require a shorter interval.

Table 4-4 is a summary of the features/configuration that the access control device is required/recommended to have.

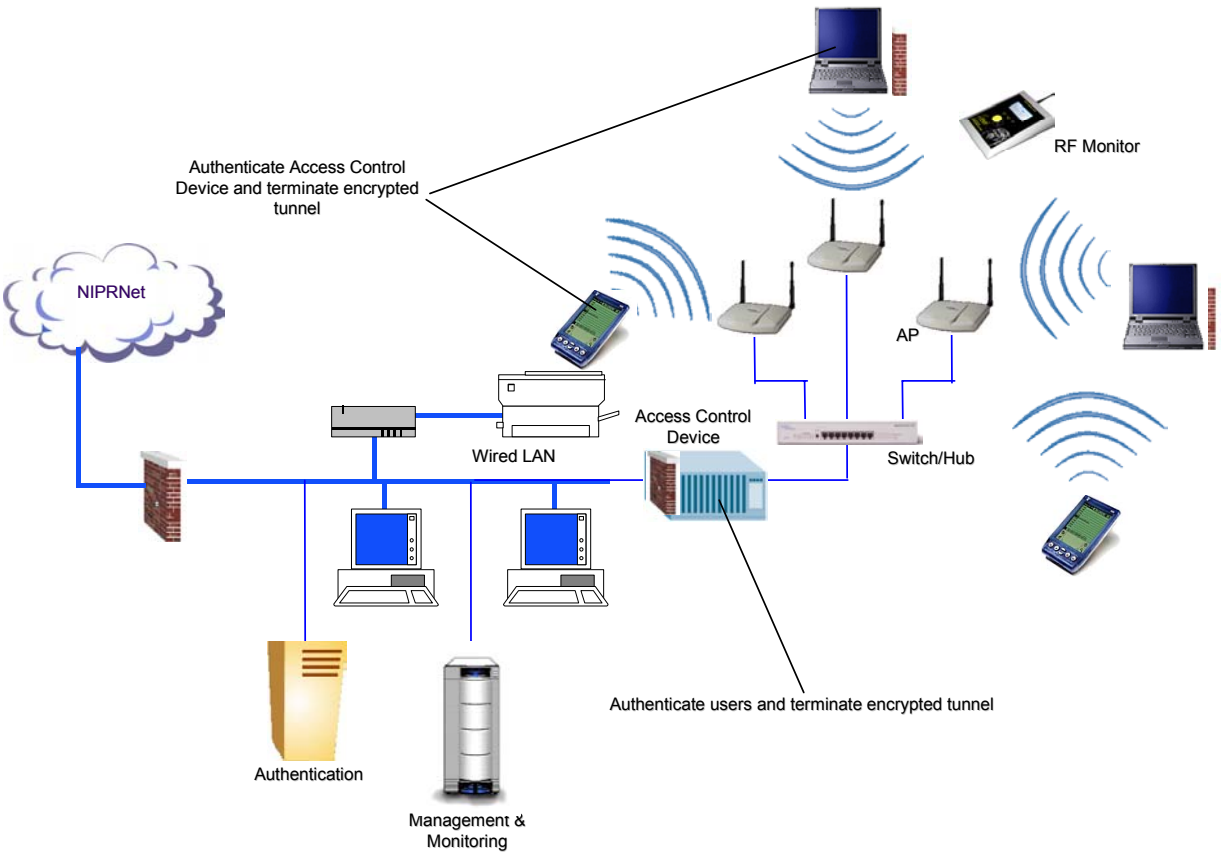
Table 4-4. Access Control Device Features/Configuration

Access Control Device Features/Configuration	Required	Recommended
Common Criteria certified against any existing Protection Profiles	✓	
Network access control (e.g., integrated firewall)	✓	
Authentication functionality	✓	
Encrypted tunneling capability (FIPS-140-2 certified)	✓	
Audit logging capability	✓	
Session time-out set to 15 minutes or less (per local security policy)		✓

4.1.5 Architecture

Figure 4-3 displays the generic architecture for the WLAN Security Framework.

Figure 4-3. Generic Architecture



A wireless network session will start with the wireless client establishing a connection with an access point within range. The negotiated session will be 128-bit WEP or WPA enabled. Further, if implemented, the access point will verify the client's MAC address to ensure it is authorized to access the network.

At the same time, the RF monitor will detect the presence of the client and the access point and log appropriate audit information (i.e., MAC addresses, date/time detected). If the RF monitor detects any unauthorized MAC addresses, the event will be logged and a system administrator alerted as soon as possible (e.g., pager, e-mail). This alert mechanism could be accomplished by connecting the RF monitor with the local Network Operations Center (NOC).

The switch/hub is not required for any security functions in this architecture; it is simply a pass-through device.

The client will then authenticate itself with the access control device. The credentials in this transaction should be either certificate- or two-factor-based. The access control

device will consult the authentication server for verification of the user's credentials and to provide authorization details.

Regardless of whether the provided credentials are valid, appropriate audit information (credentials, MAC address, date/timestamp) shall be logged by the authentication server.

After authentication is complete, an encrypted tunnel will be generated between the access control device and the wireless client. The tunnel will be terminated at those devices and not extended to other devices.

At this point, the wireless client has a secure connection to the internal network and should have access to any resources for which it has been authorized.

For all LAN activity, a network intrusion detection system will monitor the network for suspicious traffic (i.e., possible attack scenarios including port scans, denial of service /syn floods). In addition, it will verify system integrity (e.g., system file changes) and log any auditable events.

4.2 VIRTUAL PRIVATE NETWORK IMPLEMENTATION

This implementation uses a VPN device as the access control device discussed in the generic architecture.

VPNs have become a popular technology for securing network traffic over the Internet. They are commonly used for remote user access and network-to-network communication. VPNs support a number of security mechanisms:

- **Tunneling—** Allowing a device (a.k.a. tunnel endpoint) to transmit packets containing sensitive data across a public, unsecured network encapsulated within another packet for protection, usually via encryption. The outer packet is passed in the clear and contains all of the routing information a public network needs to deliver the packet to the desired network address (another tunnel endpoint). Once the complete packet is safely delivered to the trusted network device, the outer packet is shed and the inner packet is decrypted and routed to its intended destination.
- **Authentication—** Ensuring all tunnel endpoints can verify each other's identity. See Section 7.3 for additional information on authentication.
- **Access Control—** Determining what users and devices have permission to access the network as well as which individual resources should be made available. This determination is usually made using three factors: the identity of the requesting user and device, the resources requested by that user, and the predetermined access rules.

- **Data Security—**Including strong encryption and data integrity to guard against network attacks, including information tampering and capturing.

VPNs can be implemented in hardware or software using, for example, the Internet Protocol Security (IPSec) protocol suite. IPSec is an Internet Engineering Task Force (IETF) standard for providing secure communication over Internet Protocol (IP) networks. However, there are other protocols available for VPNs.

4.2.1 VPN Device

All of the components discussed in Section 4.1 are applicable to this implementation.

A VPN device will fulfill the role of the access control device. A VPN gateway or concentrator falls into the category of a VPN device. In any case, the VPN device must meet all requirements listed in Table 4-5.

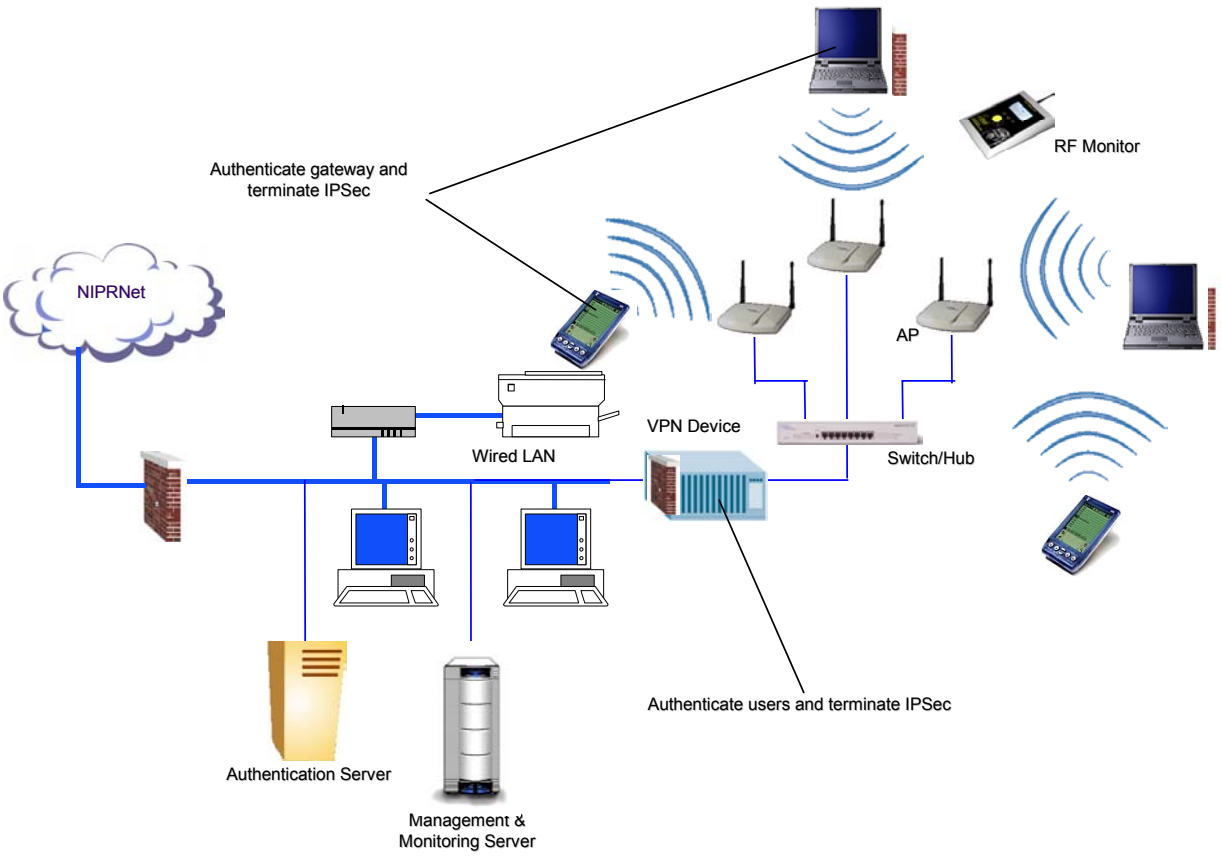
Table 4-5. VPN Compliance with Access Control Device Requirements

Access Control Device Features/Configuration	VPN Device Features
Common Criteria certified against any existing Protection Profiles	Some products are certified and some are not. Be sure to verify certification if applicable.
Network access control (e.g., integrated firewall)	VPN access control. Depending on the specific product chosen, a supplemental network firewall may be required.
Authentication functionality	VPN authentication (IPSec)
Encrypted tunneling capability (FIPS-140-2 certified)	VPN tunneling and data security (IPSec ESP tunneling). Ensure encryption is FIPS-140-2 certified.
Audit logging capability (DOD 8500.1/2 compliant)	Vendor-specific. It is recommended that a fully configurable auditing capability be available.

4.2.2 Architecture

Figure 4-4 displays the architecture for the VPN implementation.

Figure 4-4. VPN Implementation Architecture



In this implementation, a VPN tunnel is generated between the wireless client and the VPN device. During the tunnel construction, both the authentication and encryption algorithms will be negotiated and executed. The tunnel must be terminated at those devices and not extended to other devices.

4.2.3 Benefits and Limitations

The VPN implementation has a number of benefits. It is very scalable in terms of the number of clients it can service. The only client limit would be vendor implementation-specific.

Further, because VPNs are normally implemented at Open Systems Interconnection (OSI) layer 3 (network layer), they can support a number of upper layer protocols (e.g., Transmission Control Protocol [TCP], User Datagram Protocol [UDP]) and therefore a wide variety of network applications.

Per Draft DoDD 8100.2 (4.4), IPSec VPN technology must be used for WLANs supporting joint operations.

VPNs should have a relatively low Total Cost of Ownership (TCO). Because VPNs are based on an open standard, a number of vendors have products available. Hence, the competitive market should be an advantage to the buyer.

4.3 WIRELESS SECURITY GATEWAY IMPLEMENTATION

This implementation uses a Wireless Security gateway as the access control device discussed in the generic architecture.

Wireless Security gateways have been made available by a number of vendors, providing similar functionality to VPNs (see Section 4.2) specifically for WLANs. The security mechanisms offered can be a mix of standards- and proprietary-based. Depending on the vendor, encrypted tunneling can be provided at different OSI network layers.

Each gateway can support a number of access points, either directly or via switching or hubbing. For further scalability, a number of gateways can be deployed for a single WLAN to provide redundancy, fail-over protection, and seamless roaming. To manage an infrastructure with multiple gateways, vendors usually offer a centralized gateway management server to facilitate administrative tasks.

Wireless user devices will need to have a client software package installed to communicate with the gateway. Client software is normally available for a number of devices including laptops, personal digital assistants (PDA) and barcode scanners. Once the package is installed, minimal (if any) configuration is required to use the secure network.

4.3.1 Wireless Security Gateway

All of the components discussed in Section 4.1 are applicable to this implementation.

Specifically, a Wireless Security gateway will fulfill the role of the access control device. The gateway must meet all requirements listed in Table 4-6.

Table 4-6. Wireless Security Gateway Compliance with Access Control Device Requirements

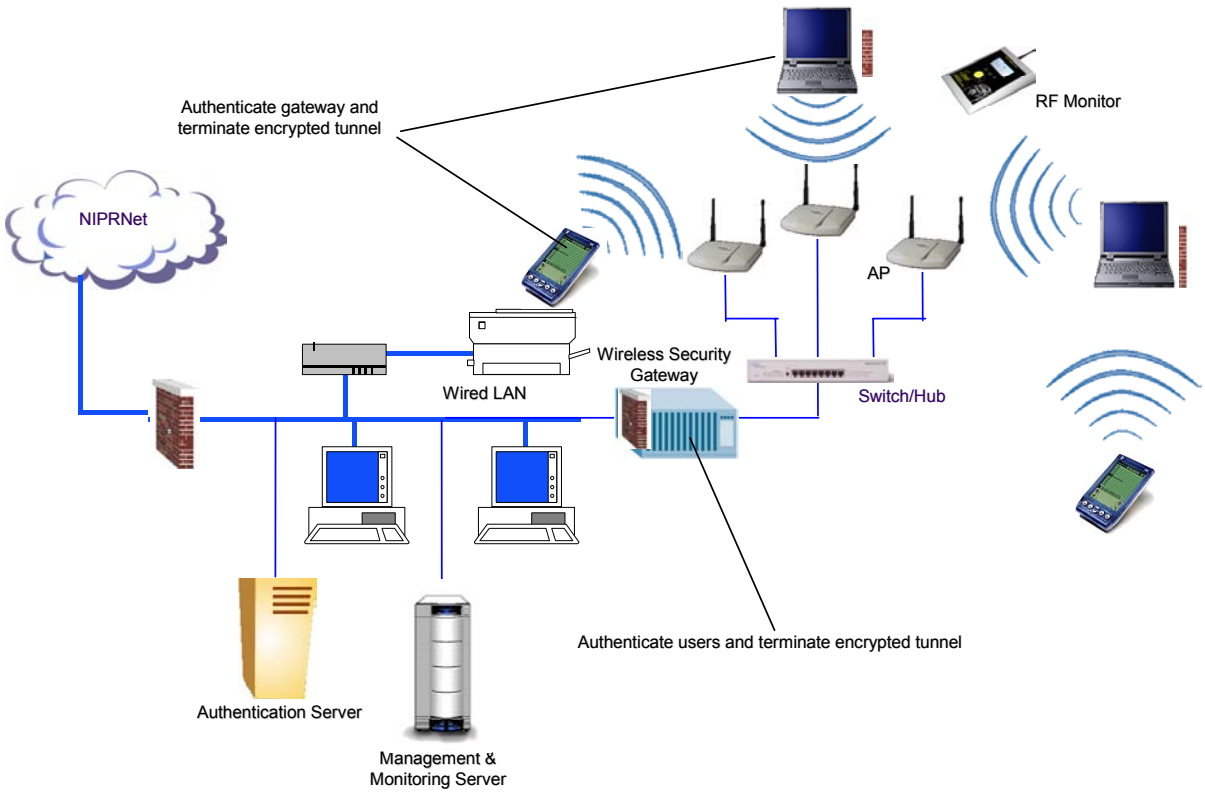
Access Control Device Features/Configuration	Wireless Security Gateway Features
Common Criteria certified against any existing Protection Profiles	Some products are certified and some are not. Be sure to verify certification if applicable.
Network access control (e.g., integrated firewall)	Vendor-specific. Depending on specific product chosen, a supplemental network firewall may be required.
Authentication functionality	Vendor-specific. Preferably a standard authentication protocol is used (e.g. EAP).
Encrypted tunneling capability (FIPS-140-2 certified)	Vendor-specific.

Access Control Device Features/Configuration	Wireless Security Gateway Features
Audit logging capability	Vendor-specific. It is recommended that a fully configurable auditing capability be available.

4.3.2 Architecture

Figure 4-5 displays the architecture for the Wireless Security gateway implementation.

Figure 4-5. Wireless Security Gateway Implementation Architecture



In this implementation, an encrypted tunnel is generated between the wireless client and the Wireless Security gateway. During the tunnel construction, both the authentication and encryption algorithms will be predetermined (or negotiated) and executed. The tunnel must be terminated at those devices and not extended to other devices.

4.3.3 Benefits and Limitations

The Wireless Security gateway implementation has a number of benefits and limitations.

Most commercially available gateways offer seamless roaming across access points for wireless users. This is a great benefit for mobile users that require a large connectivity area.

Multiple gateways can be deployed for purposes of scalability and fail-over protection. However, purchasing numerous gateways can be costly.

Gateways are relatively easy to use for wireless clients. Once the network is set up, a wireless user only needs to authenticate to the network via standard login (user id/password) or certificate (e.g., common access card [CAC] and pin). Once authenticated, the user is abstracted from the underlying security and should have access to all authorized network resources.

One potential limitation for the Wireless Security gateway is interoperability. Depending on vendor implementation, proprietary rather than open standard mechanisms could be used, which may not interoperate with other vendors' systems. If multiple vendors' products will be used in implementing a WLAN, users should ensure that interoperability would not be an issue.

4.4 WIRELESS SECURITY SWITCH IMPLEMENTATION

This implementation uses a Wireless Security switch as the access control device discussed in the generic architecture.

A Wireless Security switch is similar to a wireless gateway in that it can support multiple access points either directly or via switching/hubbing. However, a wireless switch contains all of the connection handling functionality that is normally reserved for access points. This allows for use of much simpler, smaller, and cheaper access points.

Also, by moving the connection handling from the access point to the switch, functionality such as load balancing, congestion control, and subnet roaming can be effectively provided.

4.4.1 Wireless Security Switch

All of the components discussed in Section 4.1 are applicable to this implementation.

Specifically, a Wireless Security switch will fulfill the role of the access control device. The switch must meet all requirements listed in Table 4-7.

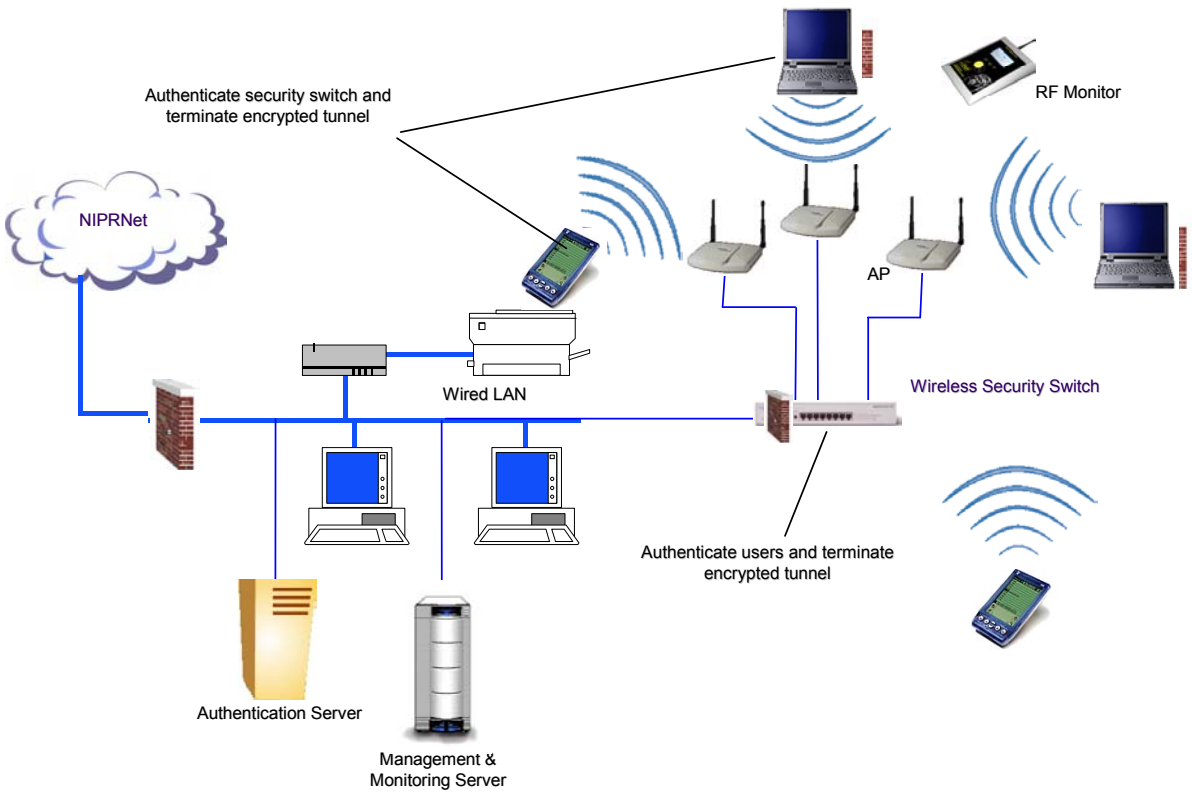
Table 4-7. Wireless Security Switch Compliance With Access Control Device Requirements

Access Control Device Features/Configuration	Wireless Security switch Features
Common Criteria certified against any existing Protection Profiles	Some products are certified and some are not. Be sure to verify certification, if applicable.
Network access control (e.g., integrated firewall)	Vendor-specific. Depending on specific product chosen, a supplemental network firewall may be required.
Authentication functionality	Vendor-specific. Preferably a standard authentication protocol is used (e.g., EAP).
Encrypted tunneling capability (FIPS-140–2 certified)	Vendor-specific.
Audit logging capability	Vendor-specific. It is recommended that a fully configurable auditing capability be available.

4.4.2 Architecture

Figure 4-6 displays the architecture for the Wireless Security switch implementation.

Figure 4-6. Wireless Security Switch Implementation Architecture



In this implementation, an encrypted tunnel is generated between the wireless client and the Wireless Security switch. During the tunnel construction, both the authentication and encryption algorithms will be predetermined/negotiated and executed. The tunnel must be terminated at those devices and not extended to other devices.

4.4.3 Benefits and Limitations

The Wireless Security switch implementation has a number of benefits. It has benefits similar to those of other implementations, such as scalability, centralized management, and roaming support.

A unique benefit is the support for simple, cheap access points. Because a number of access points are usually required for any WLAN, this could significantly lower TCO.

4.5 802.11I ROBUST SECURE NETWORK (RSN) STANDARDS-BASED IMPLEMENTATIONS

This implementation uses an RSN-capable access point or wireless switch as the access control device discussed in the generic architecture.

RSN is a major component of the soon-to-be-published 802.11i wireless security standard. Specifically, it is a total redesign of the authentication and association mechanisms used in existing 802.11 standards. Once the 802.11i standard is approved and published (expected early 2004), vendors will begin to provide devices that implement it. It is important to note that the following implementation is based on expected capabilities of RSN devices.

The RSN capability will be contained in devices at the wireless edge of the network (i.e., access points and wireless switches) rather than in devices further inside the WLAN as in the other implementations. Because of the significant changes in the security mechanisms of 802.11i, legacy access points and wireless NICs will not be upgradeable to the RSN standard. Rather, new hardware components will need to be purchased.

One potential issue with the 802.11i standard is whether RSN will be FIPS-140-2 certifiable. It is worthwhile to note that the task group responsible for 802.11i made a concerted effort to design it to be compliant with FIPS-140-2. However, if this does not occur, RSN by itself will not satisfy the encryption mechanism required by policy. However, RSN-capable access points and wireless switches would still add a layer of security to the overall architecture.

4.5.1 RSN-Capable Access Point or Wireless Switch

All of the components discussed in Section 4.1 are applicable to this implementation.

Specifically, an RSN-capable access point or wireless switch will fulfill the role of the access control device. The device must meet all requirements listed in Table 4-8.

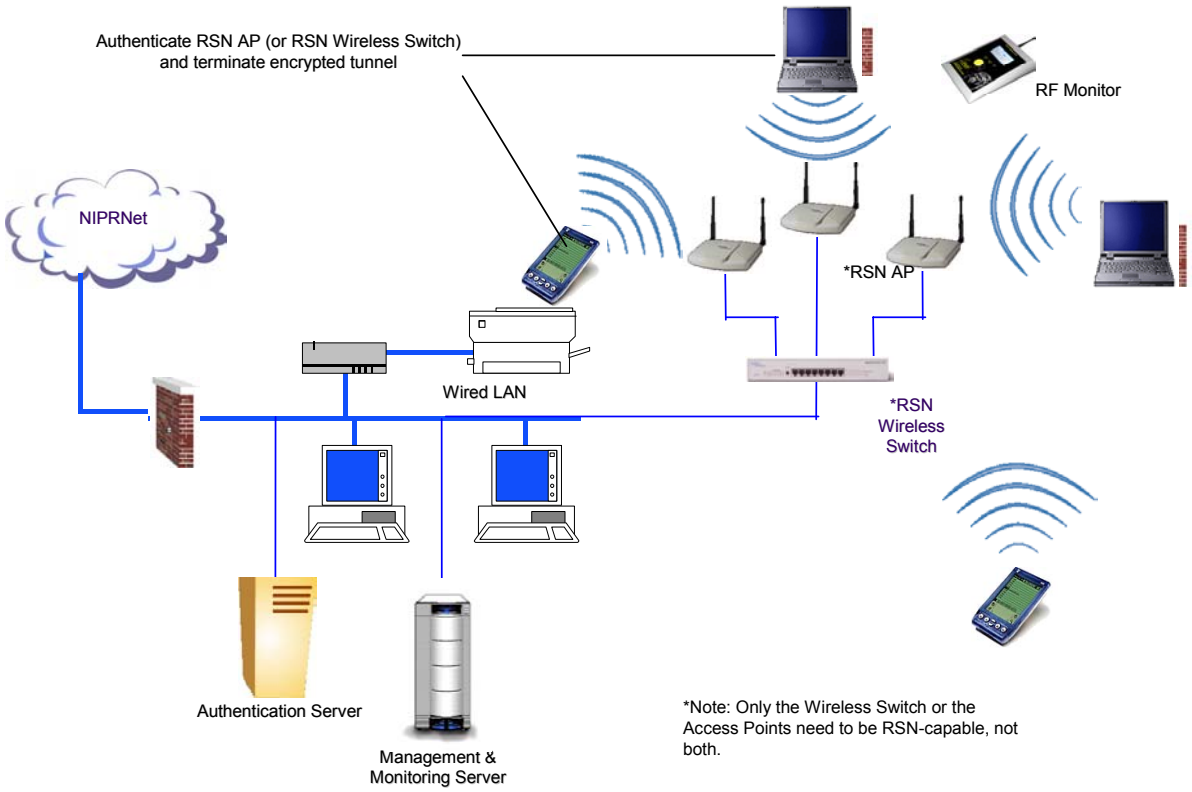
Table 4-8. RSN-capable Access Point or Wireless Switch Compliance With Access Control Device Requirements

Access Control Device Features/Configuration	RSN-capable Access Point or Wireless Switch Features
Common Criteria certified against any existing Protection Profiles	Some products are certified and some are not. Be sure to verify certification if applicable.
Network access control (e.g., integrated firewall)	Vendor-specific. Depending on specific product chosen, a supplemental network firewall may be required.
Authentication functionality	Depends on finalized standard. Preferably a standard authentication protocol is used (e.g., EAP).
Encrypted tunneling capability (FIPS-140-2 certified)	Depends on the finalized standard.
Audit logging capability	Vendor-specific. It is recommended that a fully configurable auditing capability be available.
Perform strict syntactic and semantic analysis of information provided by wireless clients	Vendor-specific. Rigorous testing should be performed to ensure no design flaws. Otherwise, attacks such as buffer overflows may be possible. See section 4.5.3.

4.5.2 Architecture

Figure 4-7 displays the model architecture for the RSN standards-based implementation.

Figure 4-7. Robust Secure Network Implementation Architecture



In this implementation, an encrypted tunnel is generated between the wireless client and the RSN-capable device. During the tunnel construction, both the authentication and encryption algorithms will be predetermined/negotiated and executed. The tunnel must be terminated at those devices and not extended to other devices.

4.5.3 Benefits and Limitations

The RSN-based implementation has a number of benefits. An RSN-capable device should have predominantly standards-based mechanisms, including strong encryption and authentication.

On the downside, upgrading existing WEP/WPA enabled wireless devices to the RSN standard will not be possible. Therefore, new access points, wireless switches, and wireless NICs will need to be purchased. Depending on the number of those components needed, this solution could be more costly than the other implementations discussed.

As noted in Table 4-8, the security of the above architecture relies on the fact that the RSN device provides thorough syntactic and semantic analysis of data provided by wireless clients. Otherwise, if the RSN device does not inspect data content, hostile wireless clients could perform buffer overflow attacks on devices on the wired LAN (e.g. the Authentication Server).

4.6 WRAP-UP DISCUSSION

The reference implementations discussed above provide models of how to implement a secure, policy-compliant WLAN. Deciding which model to follow will ultimately come down to cost factors (such as using existing assets vs. purchasing new ones) and scalability (how many access points are needed to serve the client base).

In instances where VPN components are already purchased and available, it may be best to procure some basic access points and use the available VPN device(s) for access control. FIPS-140-2 certified wireless gateways and switches are relatively new to the marketplace, therefore they probably will not be found in existing inventory. But they are also very scalable and support simple (read, cheap) access points. For WLANS supporting a large user base and requiring capabilities such as subnet roaming, these features should be attractive.

Until the 802.11i standard is published and vendors start supplying compliant products, it is difficult to forecast its relative cost factors. It should be a competitive marketplace and value should prevail for the educated consumer. However, it would appear that RSN-enabled switches would scale less expensively than RSN capable access points, especially in WLANs where a significant number of access points are required. Future revisions of this framework will follow the progress of 802.11i devices and their role in a secure, policy-compliant WLAN.

5. IMPLEMENTATION CONSIDERATIONS

This section discusses items that must be addressed and understood before implementation. Some of the major items include Common Criteria, Certification and Accreditation, policies and procedures, proprietary solutions, and scalability.

5.1 COMMON CRITERIA

The Common Criteria defines general concepts and principles of IT security evaluation and presents a basis for evaluation of security properties of IT products. It presents a common base for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. The DoD uses the Common Criteria for the procurement of commercial off-the-shelf (COTS) products for unclassified use only. Using the Common Criteria, Protection Profiles are developed to specify the security requirements desired of the product.

According to the DoDI 8500.2 policy, all information assurance (IA) products must be evaluated and validated in compliance with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 (see References) with the following qualifications:

- If there is a U.S. government Protection Profile, and there are validated products for that Protection Profile, the Government is restricted to procurement of only those products, or products that vendors have submitted, prior to purchase, for evaluation and validation to a Security Target (ST) written to that Protection Profile.
- If there is a U.S. government Protection Profile, and there are no products for that Protection Profile, the Government must require, prior to purchase, that the product be submitted for evaluation and validation to a National Information Assurance Partnership (NIAP) EVP or Common Criteria Recognition Arrangement (CCRA) lab to an ST written against that Protection Profile.
- If no U.S. government Protection Profile exists, the organization must require that the vendor provide an ST that describes the security attributes and submit their product to be evaluated and validated by a Designated Approving Authority (DAA) approved Evaluation Assurance Level (EAL).

Ideally, only Common Criteria products that are validated against a NIST or National Security Agency (NSA) Protection Profile should be used as security components in WLANs.

5.2 CERTIFICATION AND ACCREDITATION AND THE DISA CONNECTION APPROVAL PROCESS

Certification and Accreditation (C&A) is the standard DoD approach for identifying information security requirements, providing security solutions, and managing the

security of DoD information systems. In accordance with DoDD 8100.2, wireless devices, services, and technologies that are integrated or connected to DoD networks are considered part of those networks and must be certified and accredited in accordance with DoDI 5200.40. When either implementing a new system using wireless solutions or implementing wireless solutions to a previously certified system, procedures for accreditation and re-accreditation outlined in the DITSCAP should be followed. The Connection Approval Process (CAP) procedure must also be adhered to when connecting wireless to an existing system. DoD agencies can establish a CAP specific for their systems. DISA has a CAP specific for any wired and wireless connection to the S/NIPRNet. Several publications define criteria for the evaluation and validation of a system or product. Because the system or product holds a certain rating when it stands alone, it does not guarantee security when it is installed into a particular environment. The C&A of a system will take into account the systems' administration, physical security, installation, configuration mechanisms within the environment, and other security issues. It should be noted that the Certification and Accreditation of a system should be an ongoing process as software, systems, and environments are continuously evolving.

A standard process that entails all criteria should be included as the system is established and implemented. Section 11 provides a checklist that should be followed during the development and ultimately the deployment of the WLAN. Some initial actions include the identification of specific personnel positions and the development of a security policy. Within this policy, there are certain duties and parameters that should be established that cover the requirements and functionality of the operational environment and how the system will be used. As with any well-thought-out development, there must be substantial documentation. C&A as well as the CAP will require the following documentation:

- Concept of Operations (CONOPS)
- Architecture and design
- Operating procedures
- Network diagrams
- Configuration management documents
- Security incident handling process and procedures.

Along with providing documentation, various aspects of the system should be tested, including security test and evaluation (ST&E), penetration testing, and testing of the wireless network connections with documented results. If the C&A requirement and CAP is followed, the secure deployment of the WLAN will be facilitated.

5.3 POLICIES AND PROCEDURES

Currently the DoD is promoting the sharing of vulnerability mitigation strategies throughout the various DoD entities,[2]and as a result, policies have been developed to provide a balanced approach to mitigating risks in unclassified, and sensitive but unclassified environments. DoD policy[3] mandates that all wireless technologies include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques. The Pentagon[4] and various organizations within the DoD have also devised policies that are compliant with DoDD 8500 and include specific additions that relate to the respective environments. It is recommended that each local entity ensure that its local security policy is built upon and compliant with the DoDD 8500.1/2 and DoDD 8100.2.

5.4 PROPRIETARY VS. STANDARDS-BASED SOLUTIONS

There are many avenues for deploying and managing secure WLANs. The Institute of Electrical & Electronics Engineers (IEEE) has established the 802.11 standard so that users may procure interoperable products from multiple vendors to expand their network. Vendors have developed a number of proprietary security solutions because the current standards-based solutions have not proven secure. Using proprietary solutions locks users into a single vendor and leaves them at the mercy of the vendor for upgrades and bug fixes. These solutions are also immature, not interoperable, expensive, and can present numerous additional requirements for installation and maintenance.

It is recommended that agencies use tested and validated security mechanisms in network components.[5] This ensures, at a minimum, that experts have documented and verified the security of algorithms and the architecture of the mechanism. This does not mitigate all implementation-related risk but does ensure that the mechanism's foundation is sound.

5.5 SCALABILITY AND INTEROPERABILITY

The WLAN should be designed for maximum efficiency and availability and should anticipate growth of the organization. The choice of WLAN solutions will be determined based on the size and geographical distribution of the organization. There are practical aspects of mechanism deployment that are paramount to its effectiveness. The mechanism must be able to scale according to the network's needs. For example, user population can be a dynamic characteristic. As the user base grows, the security

---

2 Pentagon Area Common Information Technology (IT) Wireless Security Policy.

3 Department of Defense Instruction (DoDI) 8500.2.

4 See Pentagon Area Common Information Technology (IT) Wireless Security Policy.

5 NIST SP 800-48.

mechanisms must be able to handle the additional load such as user accounts and device management.

Current requirements may be sufficient for today's needs; however, advancements will demand a more intelligent infrastructure that will eliminate the need for adding significant infrastructure. The network designer needs to not only consider the conventional requirements but also forecast needs in the future. It is also important to implement security devices in a manner that will provide interoperability between devices in the event of network expansion. When considering scalability, agencies must recognize and ensure that networks are flexible, manageable, and standards-based.

5.6 PHYSICAL SECURITY

As network environments are becoming more complex and volatile, it is becoming imperative that organizations address the impending threat of information attacks. Maintaining strong physical security should be a critical part of any IT infrastructure.

When considering physical security, one must consider three primary control mechanisms: administrative, technical, and physical controls. If implemented correctly, these mechanisms will assist in providing a secure environment and prevent theft of network devices, and the unauthorized disclosure of information as a result of network attacks. Administrative and physical controls are similar in that they consist of the implementation of security mechanisms with respect to facility locations and layouts.

Agencies must consider the surrounding terrain and physical deterrents, such as fencing and gates, when installing wireless devices within radio communication range of the access points. Placing an access point near a public or nonsecured area would not be wise because that would give an attacker easier access to the network traffic. Agencies should also be mindful and take precautions when mounting access points and antennas to minimize their exposure to transmitters, and other potential sources of interference. It is important to be aware that, physical deterrents provide minimal levels of security, and rarely deter attackers. With the sophistication of hacking tools rising, it is not wise to rely on physical security alone to protect wireless networks.

Unauthorized individuals should be prohibited from having physical access to WLAN devices and cabling, and usage by authorized users should be monitored and logged. Isolated areas that prove to be challenging to monitor should be equipped with remote access monitoring devices manned by security personnel for monitoring purposes.

6. ADMINISTRATIVE CONTROLS

Maintaining the security of a WLAN requires constant vigilance. The network should be constantly monitored for behavior that would indicate unauthorized activity. Security administration should be established for protecting and ensuring that all security policies are being followed. There are many controls that should be used to accomplish the management's security directives as outlined in the policy. This section discusses critical administrative controls that need to be addressed in addition to technical mechanisms.

6.1 AUDITING

The auditing capability is also an essential component of a WLAN system. In a network, the system needs to be able to capture network events, also referred to as auditable events, (as defined by an administrator) and log sufficient information for analysis. There are many events that occur on a network that need to be captured to ensure that users are accountable for their actions, verify that the security policies are being enforced, and use as investigative tools. Although auditing does not deny an entity access to the network or its resources, it will track activities so a network or system administrator can assess what types of access took place, identify a security breach, or warn the administrator of suspicious activity. When implementing the audit functionality, a baseline of current activity must be established, and future activity needs to be measured against the baseline, evaluating any change from preexisting thresholds. The audited events must be analyzed against the security-risk level they present. Auditing can also be used to point out weaknesses of other technical controls and help the administrator understand changes that need to be made to preserve the necessary security level within the environment.

Audit logs contain a considerable amount of information and must be presented in an organized format. The recorded information can be organized according to system-level, user-level, and application-level events based on administrator-configured actions. The threshold and parameters of the events need to be configured by an administrator. It is not sufficient to simply gather events; the audit logs need to be monitored so that the appropriate actions can be executed.

6.2 MONITORING AND MANAGEMENT

Monitoring and management are important detective mechanisms that identify persons who attempt and succeed in gaining authorized access to the network and the information it contains. Because of the nature of RF transmissions, it is fairly easy for attackers to intrude the medium by which data traverses the network. There are different technologies for detective mechanisms, such as monitoring, that can enhance the security of the wireless link, the client, and the endpoints. Most security devices protecting wireless networks provide audit logs and alerts. Management is

commensurate with monitoring in that it is impractical to have detective mechanisms without administrators to assess the reported discovery. Monitoring mechanisms that can help identify unauthorized activity on a network enable administrators to be proactive with network security. Personnel should be designated to manage the information or alerts provided by the security devices. For example, when a user fails to login to a network because he or she is entering an incorrect password, for a configurable number of attempts, an audit log will result. Someone needs to view this information to take the appropriate action. Section 4.1.3 discusses wireless IDSs and how they are used to monitor networks. Pertinent log data should be identified, collected, and reviewed almost constantly. Products on the market facilitate the selection and prioritization of the information captured in audit logs. The monitoring capability is necessary when implementing a WLAN because a network administrator cannot monitor all the servers and network equipment constantly alone.

6.3 INCIDENT RESPONSE

Unauthorized access attempts, denial-of-service attacks, and session hijacking all represent severe attacks against a network. Although every precaution is being made to mitigate these risks, WLANs are still vulnerable to hackers. Because of this, DoD policy recommends that each location implement an incident response protocol system.

Typically a monitoring device (such as an RF monitor), alerts from an IDS, or alerts generated from the monitoring of log files can be used to detect an attack on a wireless network. Once an incident has been detected, a brief time frame is available to respond to the incident, including determining the source and possibly capturing the attacker. Therefore, it is essential that agencies establish a functional response system, and perform routine operational maintenance to control and mitigate risks. This response begins with the real-time alert mechanism of the monitoring device advising an administrator via pager, mobile phone, etc, of the event.

7. TECHNICAL MECHANISMS

Before WLAN implementation, several features should be considered that will act as countermeasures to address more specific threats and vulnerabilities. The following sections will present some of the technical mechanisms that need to be considered and implemented when designing and deploying a WLAN.

7.1 RF MONITORING

With the sophistication of WLANs and the numerous components needed to undertake the mountainous task of deploying a secure WLAN, it is essential that the network administrators be able to effectively monitor all network security components. By constantly monitoring a network, the administrators should be able to manage the entire WLAN. The robustness and integrity of a WLAN rely on the ability of the network administrator to troubleshoot problems, respond to misconfiguration, and plan for future implementations and upgrades.

There are two types of RF monitoring. One type is the act of physically driving or walking around certain areas, equipped with a sniffer to detect the presence of WLANs. Another, more effective, way is to survey wireless devices and client machines by using sensors that are strategically placed at the various components of the WLAN that report back to a centralized monitoring/management console.

Policy

According to DoD policy, measures must be implemented to monitor policy. Depending on the technology used, RF monitoring capabilities will help mitigate attacks, such as denial of service, man in the middle, and identity theft. This will satisfy the policy because the policy states that the security measures must protect not only from outside sources but also from potential attacks from friendly sources.

DoDD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG):

> 4.1.4 Measures shall be taken to mitigate denial of service attacks. These measures shall address not only threats from the outside, but potential interference from friendly sources.
>
> 4.6 The DoD Components shall actively screen for wireless devices. Active electromagnetic sensing at DoD or contractor premises to detect/prevent unauthorized access of DoD information systems shall be periodically performed by the cognizant DAA or Defense Security Service office to ensure compliance with the DITSCAP ongoing accreditation agreement (reference (e)).

Implementation

When an RF monitoring scheme is employed, it should contain the necessary mechanisms to provide a real-time network survey. The use of stationary or mobile

sensors will allow for the detection of rogue access points, ad hoc networks, and unencrypted traffic. RF monitoring can also provide the following:

- Monitoring of off-hours traffic
- Mitigation of denial-of-service attacks
- Detection of ad hoc networks
- Identification of hardware failure, network interference, slow connection speeds, and network misconfigurations

Continuously surveying the airwaves in and around the facility housing the WLAN will allow for constant monitoring of a system's components, assisting in the prevention and detection of attacks.

7.2 ENCRYPTION

The wireless link and the means by which data is transmitted are primary avenues of attack. There must be an effective way to protect information as it is stored on media or transmitted through network communication paths. The ultimate goal of encryption is to hide information from unauthorized individuals and to provide some integrity protection. Most algorithms can be cracked, yielding the protected information to be revealed, if the attacker has enough time, motivation, and resources. Thus an approach or a more realistic goal of encryption is to make the time it takes to break the algorithm so long that it is unrealistic to execute a brute-force attack.

The WEP protocol, which is used to secure the link between a wireless client and access point, was originally designed to provide security for WLANs. However, the implementation of the WEP was flawed. The Wireless Fidelity (WiFi) Alliance in conjunction with IEEE created WiFi Protected Access (WPA) as an interim solution that is interoperable and strongly enhances wireless security. WPA uses the Temporal Key Integrity Protocol (TKIP) to improve data encryption. While WPA-TKIP still uses the RC4 algorithm, a major difference is that it changes temporal keys every 10, 000 packets and with proper key management. However, WPA-TKIP is not approved for government uses because it is not FIPS 140-2-compliant.

WPA is forward compatible with the IEEE 802.11i security specification. The 802.11i Working Group has also included Advanced Encryption Standard (AES) Counter-Mode Cipher Block Chaining (CBC) Message Authentication Code (MAC) Protocol (AES-CCMP) as a part of its standard. This solution is expected to be validated by FIPS-140-2 and usable by the DoD. In the interim, the DoD must use other encryption solutions such IPSec VPNs or wireless security gateways providing FIPS-validated encryption.

When deploying WLANs, key management must be considered. Key management (the care and distribution of cryptographic keys) is the foundation for any cryptographic system. Without properly protecting cryptographic keys from unauthorized persons,

any cryptographic solution will fail to meet its objective. When deploying WLANs, distribution and management of keys must be addressed. Some solutions will use pre-shared keys; others will have a central key management infrastructure such as a public key infrastructure (PKI). Both scenarios have their strengths and weaknesses. Use of preshared keys creates a challenge in key distribution and protection of keys. A key management infrastructure such as a PKI solves much of the key management and protection problems but requires a complex infrastructure be in place. Consideration should be given to utilizing the DoD PKI when feasible and appropriate.

Policy

Per DoD policy, all encryption algorithms and protocols must be compliant with the FIPS publication 140-2. It is important to note that the WEP encryption scheme available in most 802.11 products is not FIPS-140-2 compliant. WEP's flaws are well documented, and tools that crack WEP are readily available via the Internet. Therefore, WEP encryption alone will be insufficient to satisfy the encryption requirement.

The DoDD 8100.2 policy also requires that IPSec VPN technology be used to support Joint operations.

DoDD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG):

> 4.1.2 Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the designated approving authority (DAA). At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-1 or FIPS PUB 140-2, Overall Level 1 or Level 2, as dictated by the sensitivity of the data (references (f) and (g)). Encrypting unclassified voice is desirable. PEDs shall use file system encryption. Individual exceptions may be granted on a case-by-case basis as determined by the DAA.
>
> 4.4 When unclassified wireless local area networks (WLANs) are used to support joint operations, IPSec virtual private network (VPN) technology shall be used and encrypted per subparagraph 4.1.2.

Implementation

The framework presented in this document will use FIPS-compliant algorithms, such as AES or Triple Data Encryption Standard (3DES). All key lengths, including 128, 192, 256, are of AES are adequate enough to protect classified information up to the Secret level; Top Secret requires key lengths of 192 or 256.[6] For purposes of transmitting unclassified information, AES or 3DES will still be used, because the information can be critical to the conduct and operation of organizations.

---

6 *CNSS Policy No. 15, FS-1 June 2003*

The organization can choose whether to use Layer 2 or Layer 3 encryption, or both if it is for non-Joint operations. However, IPSec will be required for Joint operations. In the future, most organizations will probably migrate to the IEEE 802.11i solution. When this happens, IPSec VPNs will be used in addition to Layer 2 encryption provided by 802.11i.

7.3 IDENTIFICATION & AUTHENTICATION

For a network to be protected against unauthorized users, identification and authentication mechanisms must be implemented. Many mechanisms exist that provide identification, authentication, and authorization when an individual connects to a WLAN. Authentication solutions include username and passwords, smart cards, biometrics, or PKI. Strong authentication will provide access control to the wired network and prevent man-in-the-middle attacks. Users connecting to the wireless network must first authenticate to the wireless network itself. In this case, the user authenticates to an access point or to some form of security gateway. Once successful authentication to the wireless network is complete and the connection is encrypted, authentication to network resources must also take place. This may include authentication to a Microsoft domain. For user-level authentication, certificate-based (e.g., PKI) or two-factor authentication is recommended.

A PKI enables users of a nonsecure public network to securely and privately exchange data through the use of a public and a private cryptographic key pair. The PKI provides for a digital certificate that contains the public key and can identify an individual or an organization that can store and revoke the certificates, if necessary.

Security token devices can also be used for strong authentication. The token device and the authentication server need to be synchronized to be able to authenticate the user. This is said to be two-factor because the token device will present the user with a sequence of characters to be entered into the computer along with an additional password.

In a wireless environment, mutual authentication shall be used to prevent attackers from masquerading as an access point or security gateway. Mutual authentication mitigates the risk that an attacker could potentially masquerade as an access point or a wireless gateway to accept and establish a connection with a wireless client. This would allow the attacker to potentially access data on the client or upload hostile code. If the authentication and authorization methods were properly implemented, the attacker would not be able to use the user credentials or brute force to establish a connection to the wired network. (Note: A attacker who inserts himself or herself in the middle of a wireless connection but does not decrypt traffic or overcome the authentication scheme is not considered a more serious threat than an attacker with an antenna and a wireless sniffer.)

Policy

According to the DoDD Policy 8100.2, strong authentication, non-repudiation, and personal identification are required for access to a DoD information system in accordance with the PKI implementation guidance. Several revised memorandums have established requirements for the use of PKI in network logon. These memos present instructions for use of PKI in DoD unclassified networks. The DoD has established the use of hardware token, certificate-based access control in the form of CAC. In accordance with the PKI memo, all DoD unclassified networks that authenticate users, unless specifically accepted by waiver, shall be PK-enabled. For many WLANs, PKI has also been deployed to provide added security.

DoDD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG):

> 4.1.1 Strong authentication, non-repudiation, and personal identification is required for access to a DoD information system (IS) in accordance with the DoD public key infrastructure (PKI) policy established by DoD Chief Information Officer (CIO). Identification and Authentication (I&A) measures shall be implemented at both the device and network level. Voice does not require DoD PKI I&A.

DoD Directive 8500.1, Information Assurance, 24 October 2002:

> 4.1 Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems in accordance with 10 U.S.C. Section 2224…
>
> 4.2 All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets…
>
> 4.8.2 The use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication shall be in accordance with published DoD policy and procedures. These technologies shall be incorporated in all new acquisitions and upgrades whenever possible. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the Department of Defense shall only accept PKI certificates obtained from a DoD-approved external certificate authority or other mechanisms approved in accordance with DoD policy.

Department of Defense (DoD) Public Key Infrastructure (PKI) Memo, 12 August 2000:

> *Enabling of Networks and Applications*: DoD unclassified networks shall be enabled for hardware token, certificate-based access control no later than October 2002, with organizations beginning this migration in December 2000, when Class 3 certificates on CACs will be available. Unclassified networks hosting mission-critical systems shall migrate to certificate-based access control using Target Class 4 tokens no later than December 32, 2003. Further guidance on enabling applications will be provided in a separate memorandum. Hardware token-based access control to classified networks is encouraged, and requirements for classified networks in this area will be provided in future guidance pending further study of technical and resource issues.

Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD) Memo, 17 May 2001:

> It is DoD Policy that:
>
> 4.1. In accordance with [the 12 August 2000 memo]:
>
> 4.1.1. All DoD unclassified networks that authenticate users, except as specified in 4.1.2, shall be PK-enabled for Class 3 hardware token, certificate-based access control conditional with the following:
>
> a. Availability of commercial certificate-based access control applications compatible with the network operating system; and
>
> b. DoD PKI issuance of access control application compatible certificates on hardware tokens (e.g., CACs) to all users of given network.
>
> Unclassified networks hosting Mission Category I systems…shall be given highest priority.
>
> 4.1.2. Unclassified DoD networks whose user communities belong predominantly to personnel categories not required to receive DoD PKI certificates in accordance with the 12 August 2000 memo] e.g., retirees, dependents, academia, are exempt from 4.1.1.

Public Key Infrastructure (PKI) Policy Update Memo, 21 May 2002:

> Certificate issuance and other [12 August 2000 and 17 May 2001 memo] requirements impacted by the revised RAPIDS fielding schedule and/or directed for completion by October 2002 are included in the following table along with revised implementation dates:

Applicable Policy	Existing October 2002 Requirement	Adjusted Milestone Date
[12 August 2000 memo, 17 May 2001 memo 4.1]	PK-enable DoD unclassified networks for hardware token, certificate-based access control	October 2003

Implementation

Current policy is that DoD PKI must be used to identify and authenticate users as they log onto networks. This neither requires nor prohibits the authentication to the WLAN device to use DoD PKI digital certificates. While authentication methods that do not incorporate DoD PKI can be used for accessing the WLAN, DoD PKI is mandated for use in identifying users as they log onto DoD networks.

In a wireless network environment, the requirements outlined in the current DoD policy memos would be satisfied if the user authenticated to the network using a digital certificate on the user's CAC, even if the user's wireless device used a different technology to authenticate itself to the wireless access point. Nevertheless, it is recommended that the CAC be used for a single sign-on authentication to the WLAN

and network resources (user logon). The DoD PKI policy memos also require the incorporation of public key technology into Web application authentication and e-mail signature and encryption. Therefore a network infrastructure that includes wireless components that will be used by individuals to access e-mail and Web servers must include the capability for those users to use their CAC to perform certificate-based authentication, digital signature, and encryption, even if the device logon or network logon is not yet using digital certificates.

Mutual authentication is necessary in a wireless environment to prevent attackers from masquerading as an access point and/or security gateway.

Note: Protected Extensible Authentication Protocol (PEAP) and Lightweight Extensible Authentication Protocol (LEAP) are not recommended as authentication mechanisms. There are known man-in-the-middle attacks that cannot be mitigated when using PEAP. PEAP's flaws are limitations in the PEAP protocol. LEAP's vulnerabilities may be able to be fixed by the vendors implementing this protocol and thus again become an authentication option.

8. MOBILE DEVICE SECURITY

Although wireless devices have commonly been regarded the weakest link in WLANs, they also have been recognized as an improvement to the mobilization of DoD infrastructures. As the popularity and feasibility of wireless devices continue to grow, the amount of users remotely accessing DoD networks has grown, which significantly broadens the network boundaries, and opens the door to numerous risks and possible attacks.

When using wireless devices to access the network, it is required that an added layer of security be implemented on the mobile device, such as personal firewalls, encrypted hard drives, and software virus protective measures.[7] This section will cover the security components required for wireless devices remotely accessing the network including PDAs, smart phones, text-messaging devices, and laptops.

8.1 COUNTERMEASURES

Mobile devices are exposed to threats inherent to a wireless environment. For example, attackers can identify and attempt to directly attack mobile devices. As a result, security mechanisms to mitigate risks must be implemented. Host-based countermeasures include the use of hardware and software solutions to facilitate securing a wireless environment and mitigating the risks associated with wireless networking. Software countermeasures include proper access point configurations, which consists of operational and security settings, software patches and upgrades, authentication, and IDS. Hardware solutions include access control devices such as VPNs, wireless gateways, and wireless switches.

8.1.1 Authentication

When implemented correctly, authentication solutions provide a reliable way of ensuring network access to authorized users only. DoD policy mandates personal identification for access to the network, and authentication measures must be implemented at the device level in addition to the network level.[8] Required solutions include the use of usernames and passwords specifying required password characters, password expiration, and minimum password length.

8.1.2 Personal Firewalls

Personal firewalls are software-based solutions that reside on a client's machine and are either client-managed or centrally managed. Client-managed versions are best suited to low-end users because individual users are able to configure the firewall themselves

7 Defense Information Systems Agency (DISA), *Secure Remote Computing Security Technical Implementation Guide (STIG).*

8 *DoD Directive 8100.2, 4.1.1.*

and may not follow any specific security guidelines. Although personal firewalls offer some measure of protection, they do not protect against advanced forms of attack. Depending on the security requirement, agencies may still need additional layers of protection. Personal firewalls also provide additional protection against rogue access points that can be easily installed in public places.

Personal firewalls are now considered to be a requirement on all remote access devices that are accessing a DoD system.[9]

8.1.3 Encryption

Encryption software can be used to protect the confidentiality of sensitive information stored on handheld devices and mirrored on the desktop personal computer (PC). The information on add-on backup storage modules should also be encrypted and the modules securely stored when not in use. This additional level of security can be added to provide an extra layer of defense to further protect sensitive information stored on handheld devices. Keeping in mind that if the information is sensitive, the encryption implementation is required to be FIPS 140-2 validated.[10]

8.1.4 Virus Protection

DoD policy suggests the use of anti-virus software for all handheld devices. Virus applications should enable users to perform routine automatic scanning of e-mails and data files. Each DoD entity with independent wireless security policies should ensure that all remote devices contain the most recent vendor supported anti-virus software. The software must be configured to ensure that the user will be prompted to update the virus signatures on a continuous 14-day basis

8.2 POLICY

According to DoD policy 8500.bb, wireless devices shall not be used or brought into a classified environment. The policy also emphasizes that wireless devices are not to be used to store, transmit, or process information where classified information is electronically stored. Policy directives specifically related to wireless devices are listed below.

DoD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG):

> 4.2. "Cellular/PCS and/or other Radio Frequency (RF) or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written

9 Defense Information Systems Agency (DISA), *Secure Remote Computing Security Technical Implementation Guide (STIG).*

10 *NIST SP 800-48.*

approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA)."

4.3. Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA, in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.

4.5. DAAs shall ensure that wireless personal area network capability is removed or physically disabled from a device unless FIPS PUB140-1/2-validated cryptographic modules are implemented (references (f) and (g)).

4.8. PEDs that are connected directly to a DoD-wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly while directly connected.

4.9. Anti-virus software shall be used on wireless-capable PEDs and workstations that are used to synchronize/transmit data. The network infrastructure shall update anti-virus software for all applicable PEDs and their supporting desktops from a site maintained by the Defense Information Systems Agency.

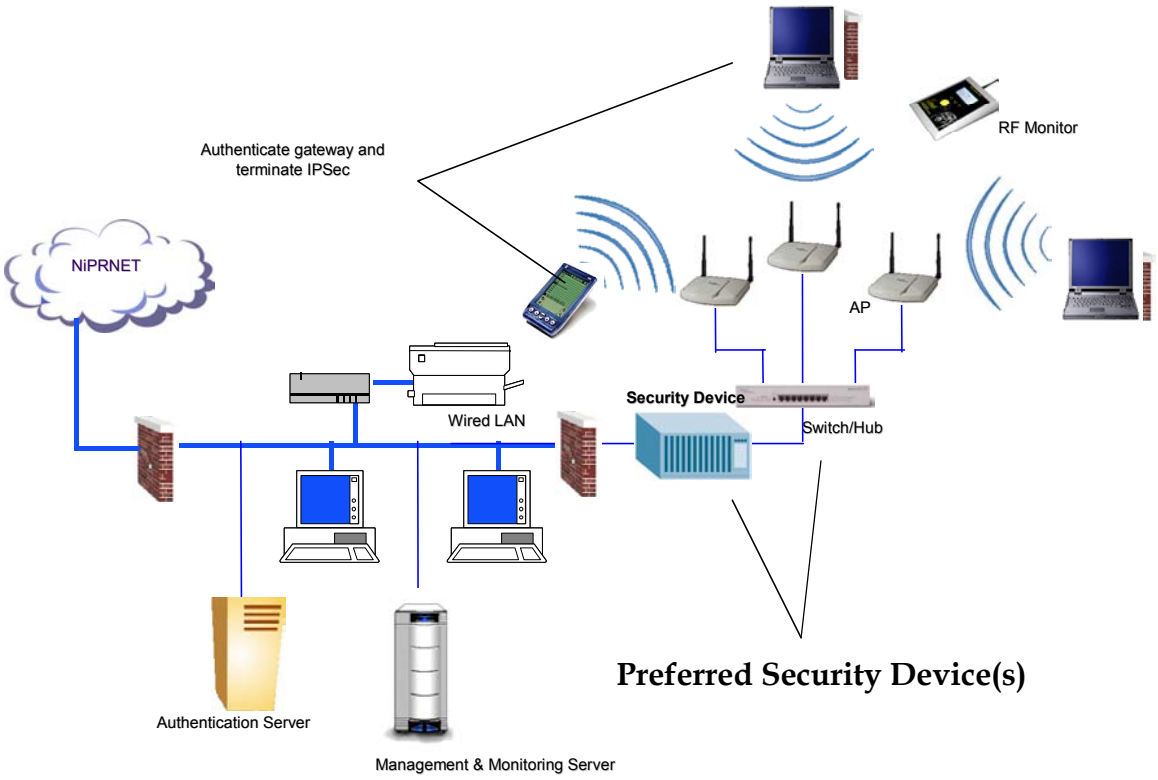
9. FUTURE CONSIDERATIONS (802.11I)

The 802.11i RSN standard is nearing its completion. All DoD wireless network managers need to include 802.11i migration in their future plans. The 802.11i standard is currently in draft form but is expected to ultimately be the architecture of choice for securing wireless networks in an unclassified environment.

10. CASE STUDIES

Wireless networks have been implemented in various DoD settings to increase user mobility and productivity levels. This section provides case studies that are based on survey data received from DoD entities, healthcare providers, and private organizations. Several technologies are currently being implemented in the field to secure WLANs. While WLAN solutions may vary according to network requirements and organization needs, the general WLAN security architectures are similar. Figure 10-1 depicts a generic wireless security solution. The general framework depicted is similar to all solutions and mirrors the WLAN framework discussed in previous sections. The selection of WLAN security components is based on several factors such as cost, user capacity, and the physical environment. However, regardless of which components are selected, if implemented properly, an adequate level of security can be provided.

Figure 10-1. Generic Wireless Security Solution



This section includes a discussion of applicable field implementations from the survey data provided, which has assisted in the formation of case studies providing secure wireless solutions including wireless gateways, switches, and VPN solutions. Some of the entities depicted include the DoD medical health services sector, the U.S. military tactical battlefield operations unit, the Engineering Logistics Center (ELC), and the

Defense Commissary Agency (DeCA), all of the case studies described within this document are equipped with FIPS 140-2 compliant encryption components.

10.1 ORGANIZATION A: DOD MEDICAL HEALTH SERVICES

10.1.1 Overview

The healthcare market has seen a tremendous increase in the demand for patient quality assurance, ranging from accidental death prevention to elevated levels of privacy assurance. Many healthcare facilities have deployed wireless networks, providing physicians and hospital staff with remote access to patient records. This allows for real-time patient monitoring resulting in better patient care.

The implementation of wireless applications has opened the doors to security challenges including intrusions and network attacks. Attacks inhibit patient privacy, thereby allowing for violation of the Federal Health Insurance Portability and Accountability Act (HIPAA), which requires that all hospitals implement security measures to protect patient information including wirelessly transmitted data. In the DoD, patient information can be a source of human intelligence and must be guarded.

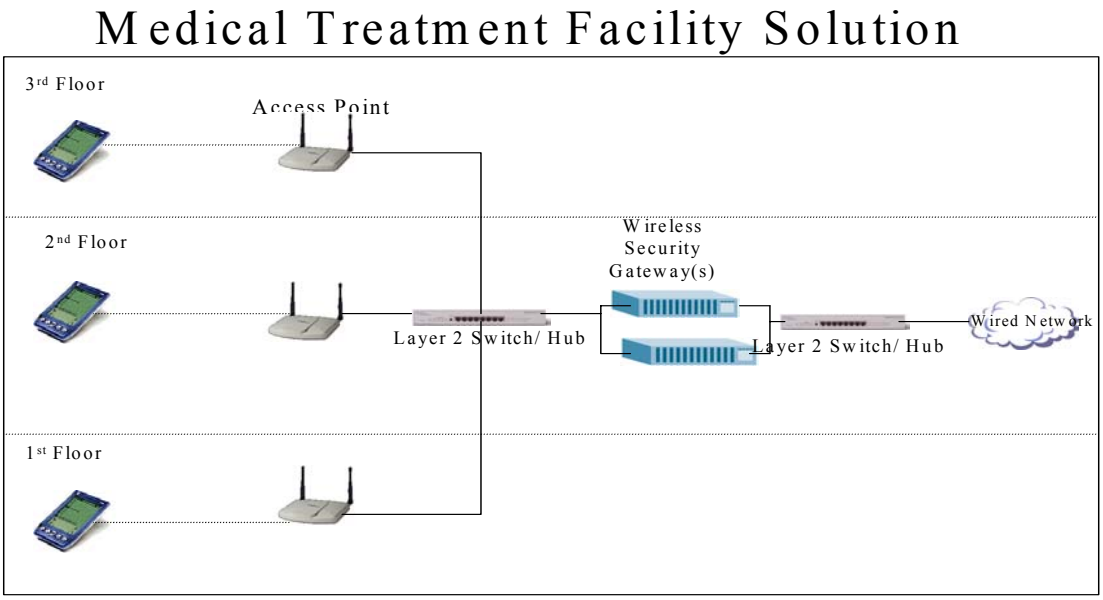
10.1.2 Solution

Within the DoD Medical Health Services unit, a strategic approach has been taken to secure the medical networks and wireless communications in various hospitals and medical centers. The security products used have been compliant with healthcare and government standards mandated by NIST and the DoD.

At one treatment facility, wireless barcode scanners were used to read patient wristbands that corresponded to patient charts and medications. The barcode scanners were connected via serial ports to tablet and/or laptop PCs configured with 802.11 NICs. The 802.11b access points were placed throughout the facilities and directly wired into a virtual local area network (VLAN) through a network switch/hub. Connected to the switch were two wireless security gateways acting as a primary and backup, which were configured into a "fail-over" mode. The two devices functioned as a bridge between the main IT network and the encrypted VLAN.

In this instance, the access control server, identified in Figure 10-2, manages device and user authentication. The control server manages the security gateways and can be tied into future policy servers, i.e., Remote Access Dial-in User Server (RADIUS) and NT domain.

Figure 10-2. Medical Treatment Facility Solution



10.1.3 Benefits

Health services within the DoD have benefited from the implementation of a secure wireless system. Physicians and hospital staff now have the ability to receive real-time information across a secure wireless network that ensures patient confidentiality.

10.2 ORGANIZATION B: SECURE COMBAT INFORMATION SYSTEM

10.2.1 Overview

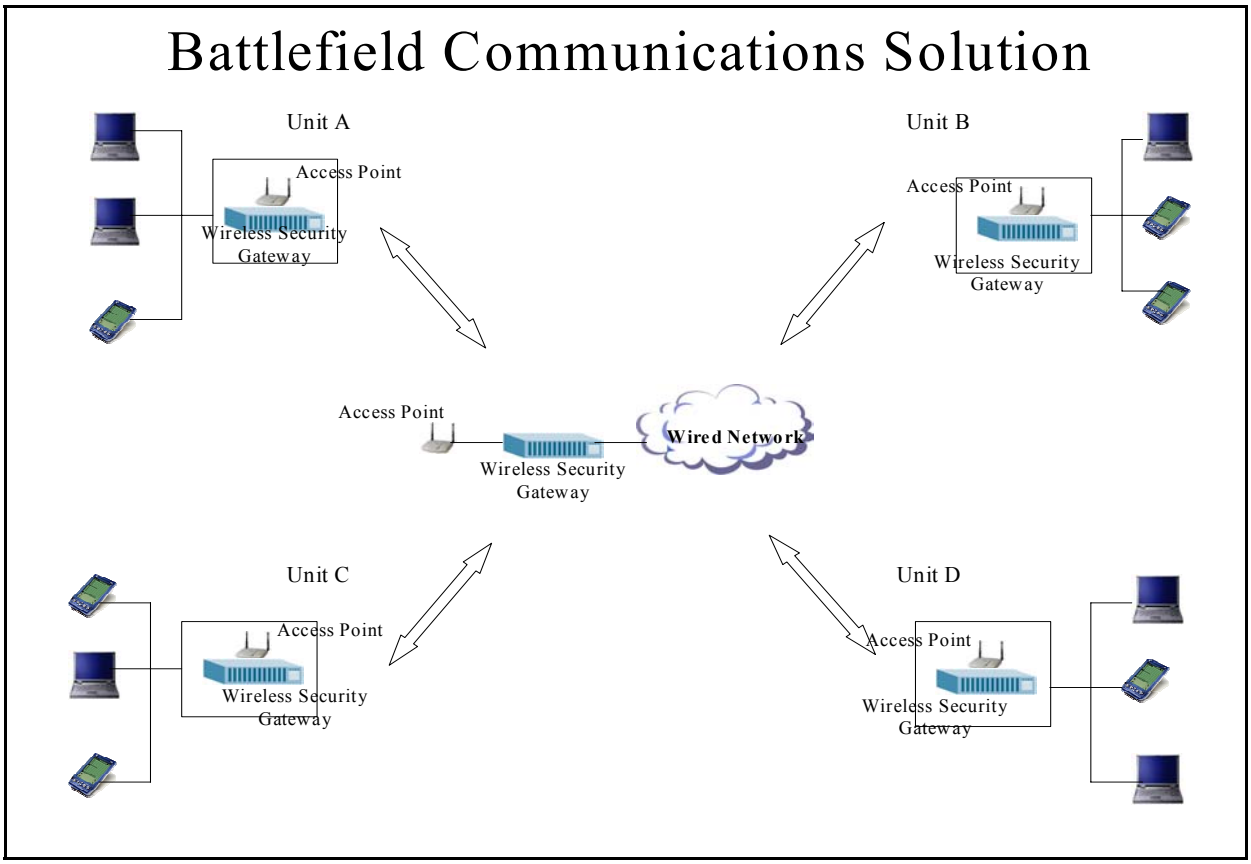
The military has improved its communication system by implementing wireless technology. This has reduced message travel time on the system, which benefits personnel with real-time information.

10.2.2 Solution

FIPS 140-2-validated wireless security gateways have been deployed to secure the tactical WLANs currently supplying military personnel with real-time information. Battlefield operations are generally outfitted with multiple tactical units including strategically placed warehouses, command facilities, and artillery units. Each tactical unit has been outfitted with PCs and/or wireless handheld devices that have been configured to authenticate to corresponding access points. At this point users/devices are identified for authentication, and data packets are encrypted. The data is then passed from the gateway through an access point to a shared access point on the

network side. Traffic is then routed from the network access point to a security gateway that decrypts the data on the wired network. (See Figure 10-3)

Figure 10-3. Battlefield Communications Solution



The security device deployed in this instance has provided a wide assortment of security and implementation features. The wireless gateway was selected mainly because of ease of use and scalability advantages. In this instance, the gateway also has the capability of providing three levels of authentication including device, user, and network authentication.

Data packets traveling between the handheld devices or PCs to the access points are WEP-encrypted. Although WEP is typically used to encrypt information between wireless access points and NICs, the vulnerabilities of WEP-enabled access points are well known and recognized within the DoD. Because WEP encryption algorithms have not been FIPS 140-2-validated and do not meet the minimum government policy requirements, AES algorithms have been implemented as reinforcement to encrypt the data packets traveling between the individual tactical units and the wired network, by way of the wireless gateway device.

10.2.3 Benefits

By implementing a secure wireless LAN, tactical units have now increased their mobility and decreased the concern of physical boundaries when positioned on the battlefield. Military personnel have now been able to eliminate the time-consuming method of using messengers to relay messages between multiple units; instead, personnel now receive real-time information.

10.3 ORGANIZATION C: ENGINEERING LOGISTICS CENTER

10.3.1 Overview

Warehouse management systems play a vital role in military/defense processes. They provide essential services to military and civilian entities, including shipment processing, packaging, and inventory maintenance. Therefore, it has become imperative that warehouses maintain efficient procedures to minimize inaccuracies, and maintain planned production levels.

Former methods have consisted of workers manually capturing and logging data. This method had become cumbersome, time-consuming, and prone to an infinite number of errors. Warehouse management centers throughout the military have reconfigured their systems to implement secure wireless solutions; this has allowed for manual operations to be replaced with automated tracking technologies.

10.3.2 Solution

Warehouse workers have been using Portable Data Terminals (PDT) with barcode scanning capabilities to scan items to be processed within the warehouse. A client is imbedded into each PDT and is assigned a device ID that is registered on the wired side Access Control Server (ACS). Each user is assigned to only one PDT; however, the PDT can support multiple users. The WLAN server also serves as a platform to the ACS, which monitors and controls the applications supplied by the wireless gateway.

The client software (corresponds to the wireless security gateway) encrypts the captured data that then travels to the access points strategically placed throughout the warehouse, via 802.11b communication over 2.4 GHz. The prior solution operated at a proprietary frequency of 900 MHz; the system has now been standardized and meets government policies at 2.4 GHz. The corresponding access points are connected to the WLAN switches via TCP/IP communication and CAT-5 cabling. The information is then routed through the wireless security gateway and the data is decrypted. AES 192-bit encryption algorithms encrypt the data packets traveling between the clients (access points) and the wireless gateway.

10.3.3 Benefits

The use of bar-coding and wireless collection terminals has increased levels of productivity and decreased the amount of errors incurred when logging information manually. Ideally this mechanism will be implemented throughout warehouses in the DoD. This alone would raise the bar for the implementation of emerging wireless technologies to further enhance production levels, and significantly cut costs.

10.4 ORGANIZATION D: DEFENSE COMMISSARY AGENCY

10.4.1 Overview

The DeCA manages more than 200 stores and distribution centers worldwide and has been using wireless technologies for some time. It was noted that security protocols were of high priority when hackers began penetrating the firewalls and compromising the DoD network. By penetrating the system, hackers were able to view patrons' sensitive information, such as credit card data, addresses, and driver's license information. During this time WEP encryption was used to encrypt data links traveling between the client and the access points. Since then WEP has not met the minimum government standard and has been deemed inadequate by NIST.

10.4.2 Solution

Within the majority of its locations, the commissary agency has begun deployment of secure wireless networks. Commissary employees are now using handheld barcode scanners equipped with client software to perform remote price checks and real-time adjustment of inventory.

Access points are placed throughout each store and distribution facilities, the access points correspond to handheld terminals (HHT) (loaded with client software), and wireless point of sales registers. The access points are routed into a VLAN on the RF/secure side of the security device via CAT-5 cabling. The security device has a nonsecure connection to the store router, which operates on a separate LAN with a different IP address block. The wired portion of the store is connected to a second router port and uses a different address block. Centralized management servers were implemented on the network to control store security devices at each location. The devices are identified and authenticated through each server by MAC addresses.

The current system meets all government requirements and is FIPS-validated featuring 3DES, and device authentication on the ACS.

There are future plans to install routers at each commissary location. The agencies are also currently deploying a wireless IDS and centralized management technology. This system will consist of passive RF sensors tied into the wired portion of the store network. The sensors report back to centralized management appliances. Each user

will be required to authenticate using a user ID and password prior to gaining access to the LAN/WAN. This added feature will be implemented with the development of a wireless edge authentication system.

10.4.3 Benefits

Because commissary employees now have access to an 802.11b secure wireless network, they are able to ensure patrons' privacy while maintaining a high level of service and production quality.

11. CHECKLISTS

When setting up a new IT system, such as a WLAN, checklists are valuable as tools during the design and engineering stages. The following checklists are included in this section:

- A Certification and Accreditation checklist is provided, which presents the steps that must be taken as a part of the design and implementation of a WLAN to have a secure system that is approved for use.
- A product selection checklist is provided that includes key components that each of the security products used in a WLAN must support.
- A WLAN Security Checklist from the NIST Special Publication 800-48 is included. This checklist provides detailed management, technical, and operational recommendations that should be addressed as a part of any WLAN design and implementation.

11.1 CERTIFICATION, ACCREDITATION AND CONNECTION APPROVAL CHECKLIST

The following checklist, Certification and Accreditation and Connection Approval Process, presents the steps that must be taken during the design and implementation of a WLAN to have a secure system that is approved for use.

Certification, Accreditation, & Connection Approval Process	
Use DoD Instruction 5200.40, DITSCAP, December 1997; DoD8510.1-M, DITSCAP Application Manual, July 31, 2000; and this checklist when implementing a new system using wireless solutions or when implementing wireless solutions to a previously certified system. http://iase.disa.mil/ditscap/ditsdocuments.html	
1. Identify the following personnel: • Designated Approving (Accrediting) Authority • Certification Authority (CA) • User Representative • Information Systems Security Officer (ISSO),	
2. Develop a security policy	
3. Determine accreditation goals and objectives A. Determine security mode of operation 1. Determine data sensitivity and classification levels 2. Determine user clearance levels 3. Determine user authorizations B. Determine the accreditation boundary (what is being reviewed, certified, and accredited) C. Determine which mission assurance category the system falls within (See DoD Instruction 8500.2, February 2003)	
4. Define the proposed operational environment and how the system will be used	
5. Develop a CONOP for the system	
6. Develop architecture and design documents including system specifications	

Certification, Accreditation, & Connection Approval Process	
7. Develop administrator and user manuals	
8. Develop operating procedures	
9. Develop network diagrams	
10. Develop configuration management documents	
11. Develop a security incident handling process and procedures	
12. Complete DoD 8510.1-M, Appendix 2 checklists Complete system architecture analysis Complete software, hardware, and firmware design analysis Complete Network Connection Rule compliance analysis Complete integrity analysis of integrated products Complete system design document Complete life-cycle management analysis Complete vulnerability assessment Complete ST&E checklist Conduct penetration testing Determine COMSEC protective measures Conduct system management analysis Perform a site accreditation survey Evaluate the contingency plan Conduct risk management review	
13. Develop/update the SSAA and appendices in accordance with DoD 5200.40	
14. Test the wireless network's • Connection to end-user devices, access points, and connection to other systems • Compliance with wireless security checklist requirements • Compliance with wireless STIG requirements	
15. Document results of test including vulnerabilities	
16. Finalize SSAA and appendices	
17. Submit SSAA to DAA for approval	
18. Modify the security policy as appropriate	
19. Submit for NIPRNet connection A. Contact the NIPRNet Product Manager or the NIPRNet Customer Service Representative to obtain information regarding the NIPRNet and procedures for connection to the network. Questions regarding the CAP and waiver process should be directed to the NIPRNet CAP Manager. Points of contact: NIPRNet Product Manager (C) (703) 882-0158, (D) 381-0158 brewera@ncr.disa.mil NIPRNet Customer Service Representative (C) (703) 882-0159, (D) 381-0159 ncgoughb@ncr.disa.mil NIPRNet CAP Manager (C) (703) 882-0133, (D) 381-0133 o'haram@ncr.disa.mil B. Access the CAP Web site, located at http://cap.nipr.mil/index.cfm, and click YES for Agreement to Monitor. C. Select CAP Registration, which will take you to http://cap.nipr.mil/capweb/cap_insert/capformpage1.cfm D. Select "Submit a new CAP" E. To register the user with the Network Information Center and identify his or her point of contact (POC) for Domain Name Service at the NIC Web page: http://www.nic.mil or call 1-800-365-3642/703-676-1051.	

11.2 PRODUCT SELECTION CHECKLIST

The following checklists include key components that each of the security products used in a WLAN must support. These checklists are also found in Section 4 but are consolidated here for clarity and convenience.

Wireless Client Features/Configuration	Required	Recommended
Common Criteria certified against any existing Protection Profiles	✓	
Applicable STIG compliance (e.g., operating system, applications)	✓	
Wireless NIC is 128-bit WEP/WPA capable.		✓
Wireless NIC is IEEE 802.1x and/or 802.11i capable (if available).		✓
Encryption client software (FIPS-140-2 certified) for storage and communication security.	✓	
Personal firewall	✓	
Intrusion Detection System (IDS)	✓	
Virus protection	✓	
File/printer sharing disabled.	✓	

Access Point Features/Configuration	Required	Recommended
Common Criteria certified against any existing Protection Profiles	✓	
128-bit WEP/WPA capability		✓
SSID beacon mode disabled		✓
Pseudo-random SSID, preferably compliant with DoD network password rules		✓
HTTP/SNMP management access disabled; ensure only secure management access is available (e.g., SSH).		✓
Transmission power set to the lowest possible setting that will meet the required signal strength for the service area	✓	
802.11i security capability (when available)		✓

RF Monitor Features/Configuration	Required	Recommended
IEEE 802.11 signal detection	✓	
Continuous scanning capability		✓
Attack signature recognition (updateable)		✓
Rogue access point /client detection		✓
MAC address ACL verification		✓
Audit logging capability		✓
Real-time alert mechanism (e-mail, pager, etc.)		✓
Integration with centralized monitoring and management systems		✓
Network health verification (e.g., interference, slow performance)		✓

RF Monitor Features/Configuration	Required	Recommended
Common Criteria certified against any existing Protection Profiles	✓	

Access Control Device Features/Configuration	Required	Recommended
Common Criteria certified against any existing Protection Profiles	✓	
Network access control (e.g., integrated firewall)	✓	
Authentication functionality	✓	
Encrypted tunneling capability (FIPS-140-2 certified)	✓	
Audit logging capability	✓	
Session time-out set to 15 minutes or less (per local security policy)		✓

11.3 NIST SPECIAL PUBLICATION 800-40 WIRELESS SECURITY LAN CHECKLIST

The following Wireless LAN Security Checklist[11] from the NIST Special Publication 800-48 provides users and implementers with detailed management, technical, and operational recommendations that should be addressed as a part of any WLAN design and implementation.

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
Management Recommendations				
1.	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	✓		
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	✓		
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	✓		
4.	Ensure that the client NIC and access point support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).	✓		
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue access points do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	✓		
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	✓		

11 NIST Special Publication 800-48

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
7.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
8.	Complete a site survey to measure and establish the access point coverage for the agency.	✓		
9.	Take a complete inventory of all access points and 802.11 wireless devices.	✓		
10.	Ensure that wireless networks are not used until they comply with the agency's security policy.	✓		
11.	Locate access points on the interior of buildings instead of near exterior walls and windows as appropriate.	✓		
12.	Place access points in secured areas to prevent unauthorized physical access and user manipulation.	✓		
Technical Recommendations				
13.	Empirically test access point range boundaries to determine the precise extent of the wireless coverage.	✓		
14.	Make sure that access points are turned off when they are not being used (e.g., after hours and on weekends).	✓		
15.	Make sure that the reset function on access points is being used only when needed and is invoked only by an authorized group of people.	✓		
16.	Restore the access points to the latest security settings when the reset functions are used.	✓		
17.	Change the default SSID in the access points.	✓		
18.	Disable the broadcast SSID feature so that the client SSID must match that of the access point.		✓	
19.	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.	✓		
20.	Ensure that access point channels are at least five channels different from any other nearby wireless networks to prevent interference.	✓		
21.	Understand and make sure that all default parameters are changed.	✓		
22.	Disable all insecure and nonessential management protocols on the access points.	✓		
23.	Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature.	✓		
24.	Ensure that encryption key sizes are at least 128-bits or as large as possible.	✓		
25.	Make sure that default shared keys are periodically replaced by more secure unique keys.	✓		
26.	Install a properly configured firewall between the wired infrastructure and the wireless network (access point or hub to access points).	✓		
27.	Install anti-virus software on all wireless clients.	✓		
28.	Install personal firewall software on all wireless clients.	✓		
29.	Disable file sharing on wireless clients (especially in untrusted environments).	✓		
30.	Deploy MAC access control lists.		✓	
31.	Consider installation of Layer 2 switches in lieu of hubs for access point connectivity.	✓		

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
32.	Deploy IPsec-based VPN technology for wireless communications.		✓	
33.	Ensure that the encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.	✓		
34.	Fully test and deploy software patches and upgrades on a regular basis.	✓		
35.	Ensure that all access points have strong administrative passwords.	✓		
36.	Ensure that all passwords are being changed regularly.	✓		
37.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.		✓	
38.	Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.	✓		
39.	Use static IP addressing on the network.		✓	
40.	Disable Dynamic Host Configuration Protocol (DHCP).		✓	
41.	Enable user authentication mechanisms for the management interfaces of the access point.	✓		
42.	Ensure that management traffic destined for access points is on a dedicated wired subnet.	✓		
43.	Use SNMPv3 and/or SSL/TLS for Web-based management of access points.	✓		
Operational Recommendations				
44.	Configure SNMP settings on access points for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.	✓		
45.	Enhance access point management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	✓		
46.	Use a local serial port interface for access point configuration to minimize the exposure of sensitive management information.		✓	
47.	Consider other forms of authentication for the wireless network, such as RADIUS and Kerberos.		✓	
48.	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.		✓	
49.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.		✓	
50.	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.		✓	
51.	Enable use of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys.	✓		
52.	Fully understand the impacts of deploying any security feature or product prior to deployment.	✓		
53.	Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.		✓	

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
54.	Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.		✓	
55.	When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	✓		
56.	If the access point supports logging, turn it on and review the logs on a regular basis.	✓		

12. ACRONYMS

3DES	Triple Data Encryption Standard
ACL	Access Control List
ACS	Access Control Server
AES	Advanced Encryption Standard
AP	Access Point
C&A	Certification and Accreditation
CA	Certificate Authority
CAC	Common Access Card
CAP	Connection Approval Process
CBC	Cipher Block Chaining
CCMP	Counter-Mode CBC MAC Protocol
CCRA	Common Criteria Recognition
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
DAA	Designated Approving Authority
DeCA	Defense Commissary Agency
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DITSCAP	Defense Information Technology Systems Certification and Accreditation Process
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
ELC	Engineering Logistics Center
EAP	Extensible Authentication Protocol
EVP	
FIPS	Federal Information Processing Standards
GHz	Gigahertz
GIG	Global Information Grid
HHT	Hand Held Terminals
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol, Secure
IA	Information Assurance
IDS	Intrusion Detection System
IEEE	Institute of Electronic and Electrical Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ISSO	Information Systems Security Officer

IT	Information Technology
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control or Message Authentication Code
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NOC	Network Operations Center
OSI	Open Systems Interconnection
PC	Personal Computer
PDA	Personal Digital Assistant
PDT	Portable Data Terminal
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
POC	Point of Contact
PUB	Publication
RADIUS	Remote Access Dial-in User Service
RF	Radio Frequency
RSN	Robust Secure Network
SNMP	Simple Network Management Protocol
SRM	Security Reference Model
SSAA	System Security Authorization Agreement
SSH	Secure Shell
SSL	Secure Sockets Layer
SSID	Service Set Identifier
ST&E	Security Test and Evaluation
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TRANSEC	Transmission Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Protocol
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access